

6-5-2014

# Assessment of users' information security behavior in smartphone networks

Mohammadjafar Esmaeili

Follow this and additional works at: <http://commons.emich.edu/theses>



Part of the [Science and Technology Studies Commons](#)

---

## Recommended Citation

Esmaeili, Mohammadjafar, "Assessment of users' information security behavior in smartphone networks" (2014). *Master's Theses and Doctoral Dissertations*. 581.

<http://commons.emich.edu/theses/581>

This Open Access Dissertation is brought to you for free and open access by the Master's Theses, and Doctoral Dissertations, and Graduate Capstone Projects at DigitalCommons@EMU. It has been accepted for inclusion in Master's Theses and Doctoral Dissertations by an authorized administrator of DigitalCommons@EMU. For more information, please contact [lib-ir@emich.edu](mailto:lib-ir@emich.edu).

Assessment of Users' Information Security Behavior in Smartphone Networks

by

Mohammadjafar Esmaeili

Dissertation

Submitted to the College of Technology

Eastern Michigan University

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN TECHNOLOGY

Concentration in Information Assurance

Dissertation Committee:

Ali Eydgahi, Chair

Huei Lee, PhD

Konnie Kustron, PhD

Alphonso Bellamy, PhD

June 5, 2014

Ypsilanti, Michigan

## **Abstract**

With the exponential growth of smartphone usage, providing information security has become one of the main challenges that researchers and information-security specialists must consider. In contrast to traditional mobile phones that only enable people to talk and text, smartphone networks give users a variety of convenient functions such as connection to the Internet, online shopping, e-mail and social media, data storage, global positioning systems, and many other applications. Providing security in smartphone networks is critical for the overall information security of individuals and businesses. Smartphone networks could become vulnerable to security breaches if users do not practice safe behaviors such as selecting strong passwords, encrypting their stored data, downloading applications only from authorized websites, not opening emails from unknown sources, and updating authorized security patches. Users of smartphone devices play an important role in providing information security in smartphone networks, which affects the information security of private and public networks.

This study assessed the factors that affect users' security behavior on smartphone networks. By reviewing the theoretical frameworks that evaluate human behavior, this study formed a research model. The research model identified attitude, intention, computing experience, breaching experience, and facilitation condition as the main and direct factors that influence information security behavior in smartphone networks. This study performed several analyses on the investigator-developed survey questionnaire to ensure validity and reliability. Examining all of the proposed direct constructs, this study found that users' facilitation condition does not have significant impact on the information security behavior in smartphones. This research also showed that gender and employment status have moderating

effects on several hypothesized paths. The findings of this research could help information-security developers to design better systems that could provide stronger information security for individuals and businesses that share their networks with users' smartphones.

## **Dedications**

I dedicate this work to my creator: Allah, the most compassionate the most merciful;

my wife: Arwa; my parents: Mohammadali and Masoumeh;

and

my brothers and sister

for unconditional and infinite love and support.

## **Acknowledgements**

I would like to express my sincere gratitude and appreciation to Dr. Ali Eydgahi, chair of my Ph.D. research, for his guidance, support, and insightful comments throughout this research.

I would also like to thank the other members of the research committee, Dr. Konnie Kustron, Dr. Huei Lee, and Dr. Alphonso Bellamy, for their valuable input and supports throughout this project.

I would first and foremost like to express my gratitude to my parents for the love, affection, and support that they have extended me at every step of my life.

I am extremely grateful to the institution, faculty, and staff at Eastern Michigan University for the support and guidance. I am also thankful to my fellow Eastern Michigan University graduate students for their friendship over the years.

## Table of Contents

|   |    |
|---|----|
| Abstract .....  | ii |
| Dedications .....   | iv |
| Acknowledgements .....                                      | v  |
| Table of Contents .....                                     | vi |
| List of Tables .....  | ix |
| List of Figures .....                                       | xi |
| Chapter 1. Introduction .....                               | 1  |
| Nature and Significance of the Problem .....                | 4  |
| Statement of the Problem .....                              | 6  |
| Objectives of the Research .....                            | 7  |
| Proposed Model .....  | 8  |
| Behavior, behavioral control, intention, and attitude ..... | 8  |
| Attitude .....  | 10 |
| Research questions .....                                    | 12 |
| Research hypotheses .....                                   | 13 |
| Limitations .....   | 15 |
| Assumptions .....   | 15 |
| Definitions of terms .....                                  | 16 |
| Summary .....   | 18 |
| Chapter 2. Review of the Literature and Background .....    | 19 |
| Introduction .....  | 19 |
| Smartphone Security .....                                   | 19 |
| Theoretical Frameworks .....                                | 20 |

|   |    |
|---|----|
| Theory of planned behavior.....                   | 21 |
| Technology acceptance model.....                  | 23 |
| Decomposed theory of planned behavior .....       | 26 |
| Fear appeals and protection motivation model..... | 32 |
| Information Security Adaptation Model .....       | 35 |
| Summary .....                                     | 36 |
| Chapter 3. Research Methodology.....              | 38 |
| Introduction .....                                | 38 |
| Research Methods .....                            | 38 |
| Population and Sampling .....                     | 38 |
| Instrument Design .....                           | 39 |
| Instrument Validity .....                         | 47 |
| Pilot Test .....                                  | 48 |
| Scale Reliability .....                           | 48 |
| Human Subjects.....                               | 49 |
| Data Collection.....                              | 49 |
| Data Analysis .....                               | 50 |
| Summary .....                                     | 51 |
| Chapter 4. Results.....                           | 52 |
| Completion Rates .....                            | 52 |
| Demographic Characteristics of the Sample .....   | 53 |
| Assessment of Measures .....                      | 55 |
| Pilot and feedback analysis.....                  | 55 |



|  |     |
|--|-----|
| Descriptive and reliability analysis.....                    | 56  |
| Normality.....   | 58  |
| Factor analysis .....  | 61  |
| Construct validity .....                                     | 68  |
| Hypotheses testing.....                                      | 72  |
| Explanation of target endogenous variable variance.....      | 72  |
| Inner model path coefficient sizes and significance.....     | 75  |
| Checking structural path significance in bootstrapping ..... | 77  |
| Moderating factors.....                                      | 85  |
| Mediating factors.....                                       | 89  |
| Summary .....  | 91  |
| Chapter 5. Discussion, Conclusions, and Implications.....    | 93  |
| Overview of the Study.....                                   | 93  |
| Discussion .....   | 94  |
| Research Conclusions .....                                   | 97  |
| Research Implications .....                                  | 100 |
| Research Limitations and Future Studies.....                 | 103 |
| References.....  | 106 |
| Appendixes .....   | 114 |
| Appendix A.....  | 115 |
| Appendix B.....  | 117 |
| Appendix C.....  | 118 |

## List of Tables

| <b><u>Table</u></b> |   | <b><u>Page</u></b> |
|---------------------|---|--------------------|
| 1                   | Constructs and Items.....                                       | 40                 |
| 2                   | Demographic characteristics of the sample.....                  | 53                 |
| 3                   | Education Level.....  | 54                 |
| 4                   | Demographic Characteristics.....                                | 54                 |
| 5                   | Respondents' feedback.....                                      | 56                 |
| 6                   | Cronbach's Alpha for constructs (N=593).....                    | 57                 |
| 7                   | Normality Analysis.....   | 59                 |
| 8                   | Factor Loading.....   | 62                 |
| 9                   | Convergent Validity.....  | 69                 |
| 10                  | Discriminant Validity Analysis.....                             | 71                 |
| 11                  | Explanation of Variable Variance Analysis.....                  | 75                 |
| 12                  | Inner Model Path Coefficient Sizes and Significance.....        | 76                 |
| 13                  | Hypothesis Testing.....   | 78                 |
| 14                  | PLS-SEM Analysis for Two Groups of Male and Female.....         | 86                 |
| 15                  | PLS-SEM Analysis for Two Groups of Employed and Unemployed..... | 88                 |
| 16                  | Mediation Factors.....  | 91                 |
| 17                  | Security Behavior Item Analysis (N=593).....                    | 120                |
| 18                  | Security Intention Descriptive Analysis (N=593).....            | 121                |
| 19                  | Security Attitude Descriptive Analysis (N=593).....             | 122                |
| 20                  | Subjective Norm Descriptive Analysis (N=593).....               | 123                |
| 21                  | Perceived Behavioral Control Descriptive Analysis (N=593).....  | 124                |

|    |   |     |
|----|---|-----|
| 22 | Perceived Usefulness Descriptive Analysis (N=593).....      | 125 |
| 23 | Perceived Ease of Use Descriptive Analysis (N=593).....     | 126 |
| 24 | Perceived Probability Descriptive Analysis (N=593).....     | 127 |
| 25 | Perceived Severity Descriptive Analysis (N=593).....        | 129 |
| 26 | People's Influence Descriptive Analysis (N=593).....        | 130 |
| 27 | Descriptive Analysis of Media's Influence (N=593).....      | 131 |
| 28 | Descriptive Analysis of Self-Efficacy (N=593).....          | 132 |
| 29 | Descriptive Analysis of Facilitating Condition (N=593)..... | 133 |
| 30 | Descriptive Analysis of Breach Experience (N=593).....      | 134 |
| 31 | Descriptive Analysis of Computing Experience (N=593).....   | 135 |

## List of Figures

| <b><u>Figure</u></b> |   | <b><u>Page</u></b> |
|----------------------|---|--------------------|
| 1                    | Factors that affect attitude.....                                 | 11                 |
| 2                    | Proposed Research Model .....                                     | 12                 |
| 3                    | Research Hypotheses.....  | 13                 |
| 4                    | Theory of Reasoned Action .....                                   | 21                 |
| 5                    | Theory of Planned Behavior .....                                  | 22                 |
| 6                    | The Technology Acceptance Model .....                             | 24                 |
| 7                    | TAM and information system security adaptation.....               | 25                 |
| 8                    | Decomposed Theory of Planned Behavior .....                       | 27                 |
| 9                    | Model of home users' intention to practice computer security..... | 31                 |
| 10                   | Security attitude and other latent variables.....                 | 35                 |
| 11                   | Smartphone information security behavior adaptation model.....    | 36                 |
| 12                   | SmartPLS path modeling results .....                              | 74                 |
| 13                   | Analysis of SEM without mediating factors.....                    | 90                 |
| 14                   | Analysis of SEM with mediating factors.....                       | 90                 |
| 15                   | Results of PLS-SEM path analysis.....                             | 94                 |

## **Chapter 1. Introduction**

The digital era connects all corners of the world together and provides people with opportunities that were not imaginable before. With the advent of the Internet, organizations have moved toward using this technology as an asset that enables their businesses. Providing information security becomes extremely relevant and required by these organizations (Kankanhalli, Teo, Tan, & Wei, 2003). In addition to the popularity of the Internet, providing security for different types of networks and avoiding information breaches are daily challenges for information system security specialists. Furnell, Bryant, and Phippen (2007) note that, “As Internet connectivity and online applications continue to increase, Internet users are becoming ever more vulnerable to security incidents, and the overall range of threats is growing at an alarming rate” (p. 410). Users of the internet are continuously facing new security threats such as viruses, worms, Trojans, phishing, and intellectual property thefts. These threats can be costly and dangerous for all online users. According to Fossi et al. (2009), the United States was the top country for overall malicious activity in 2008 and the average cost per incident of a data breach in the United States alone was \$6.7 million.

Users store their information on a variety of devices such as desktops, laptops, PDAs, tablets, and smartphones, to name a few. Among all of these technologies, smartphones are becoming one of the most convenient devices, which can connect users to the Internet and enable them to browse it, connect to social networks, send and receive emails, shop online, play games, store data, navigate with GPS, and many other functions. Due to these capabilities, “Mobile devices are becoming a critical component of the digital economy, a style statement and useful communication device, and a vital part of daily life for billions of people around the world.” (Androulidakis & Kandus, 2011a, p. 18) The analyst firm Gartner

predicts (as cited in Egan et al., 2012) that, "...the sales of smartphones to end users will reach 461.5 million in 2011 and rise to 645 million in 2012 and in 2011, sales of smartphones will overtake shipments of PCs (364 million)" (p. 13).

As a result, users tend to store considerable amounts of data, both personal and job related, in their smartphones. A survey done by Lazou and Weir (2011) revealed that, "The storage of personal information is on the rise, with 16% of people storing their bank details and nearly 25% storing PIN numbers and passwords" on their smartphones (p. 184). This sensitive information requires the same level of protection as if it were stored on other devices. Although users store extensive amounts of sensitive information on their smartphones, they generally do not take proper actions toward securing this information in their devices. Some of the key components of any device that provides connection to the Internet include hardware, software, and users. Many organizations and information-security specialists agree that providing security in organizational networks is an ongoing challenge and many researchers are looking to provide information security by improving software, hardware, and firmware. According to Arbaugh (2003), in order to provide security in information system networks, not only is there a need for appropriate security infrastructure but also users should, "Do the right thing when confronted with something out of the ordinary" (p. 100). For example, surveys done by Androulidakis and Kandus (2011a) show that 21.6% of users keep their passwords saved in plain text in their mobile phone. Hence, such a behavior could make the data stored on the smartphones an easy target for hackers.

In other words, internal users in any network play a critical role and can be a great source of risk to information systems. Security practitioners aim to achieve the three goals of confidentiality, integrity, and protected availability of information to secure an organization's

information assets (Easttom, 2006; Ramirez, 2006; Willison et al., 2006 [as cited in Lamour, 2008]). Lamour (2008) point out that, even in the absence of a purposeful human attacker or equipment failure, human error, not technology, is the primary problem in information security.

Although smartphones are extremely popular, they also are more vulnerable to security breaches, which could endanger the confidentiality, integrity, and availability of the stored data. According to Egan et al. (2012):

With the number of vulnerabilities in the mobile space rising (a 93.3% increase over 2010) and malware, authors are not only reinventing existing malware for mobile devices but are also creating mobile-specific malware geared to the unique opportunities mobile devices present. The year 2011 was the first year that mobile malware presented a tangible threat to enterprises and consumers. Mobile malware also creates an urgent concern to organizations around the possibility of breaches. Given the intertwining of work and personal information on many mobile devices, the loss of confidential information presents a real risk to businesses. Unlike a desktop computer, or even a laptop, mobile devices are easily lost. Recent research by Symantec shows that 50% of lost phones will not be returned and that for unprotected phones, 96% of lost phones will have the data on that phone breached. (p. 13)

Although a strong password, antivirus, antispysware, and other information security technologies are necessary, improving users' security behavior should be the first line of defense in securing smartphone networks, which is why this issue requires immediate attention. For instance, it would be useless if we put the most secure encryption or password systems on smartphones but then failed to teach users how to use the technologies. Thus, it is

vital to find out what the main factors are that affect users' security behaviors on mobile devices such as smartphones. This assessment would help the security specialist to focus on the methods that could improve users' security behavior, which should then eventually ensure the confidentiality, integrity, and availability of the sensitive data that has been stored on smartphones, which then would provide more information security for the networks that share their resources with these devices. In other words, by identifying the factors that affect users' security behavior, information-security experts and businesses could design systems that could educate users more effectively toward practicing security behaviors, resulting in a more robust and secure smartphone network.

The main goal of this descriptive model-testing study is to examine the relationship between the factors that impact users' secure behavior on smartphones. In other words, this study attempts to find any possible relationships among some factors such as: attitude toward practicing security behavior, intention toward practicing security behavior, subjective norms regarding practicing security behavior, and perceived behavioral control. Eventually, this research will propose a model to understand the effect of the above factors on practicing security behavior and utilizing security technologies on smartphone networks.

### **Nature and Significance of the Problem**

Furnell, Bryant, and Phippen (2007) note that, "As Internet connectivity and online applications continue to increase, Internet users are becoming ever more vulnerable to security incidents, and the overall range of threats is growing at an alarming rate" (p. 410). In today's digital era, one of the main devices that connect users to the Internet is a smartphone. Smartphones are becoming very popular and, "Mobile devices are becoming a critical component of the digital economy, a style statement and useful communication device, and a



vital part of daily life for billions of people around the world” (Androulidakis & Kandus, 2011a, p. 18). Smartphones and mobile networks are vulnerable to information security breaches and are facing new security threats such as viruses, worms, Trojans, phishing, and intellectual property thefts. These threats can be costly and dangerous for all users. As noted above, Fossi et al. (2009) found that the United States had the highest rate of overall malicious activity in 2008 at great cost to users. Lazou and Weir (2011) state, “Mobile devices are by their nature more vulnerable to theft and accidental loss than larger systems in fixed locations” (p. 183), demonstrating further that providing security for mobile networks and avoiding information breach is one of the main daily challenges of information system security specialists in smartphone networks. Not only can an unsecured smartphone device risk the security of the personal data, but also it could risk business information assets. For instance, employees who use their personal smartphone at work could pose more risk to a business’s information security (Egan et al., 2012). “Users create an open back door into our corporate networks through their Internet-enabled services, third party application use, and electronic interaction (i.e. email) with other users. This vulnerability is increased when mobile systems joined home and other commercial networks” (Dodge, Carver, & Ferguson, 2007, p. 73).

Activating security technologies could reduce the risk of security breaches on smartphone networks only if users showed enough interest to learn and utilize them. For example, smartphone networks would be vulnerable to security breaches if users did not consistently practice selecting a strong password, encrypting their stored data, downloading applications only from authorized websites, ignoring unknown emails, and failing to update authorized security patches. Users of smartphone devices play an important role in providing

information security in smartphone networks, which affects the information security of private and public networks. Not only do these vulnerable devices jeopardize confidentiality, integrity, and availability of individuals' sensitive data but they also expose any networks that they use to connect to the Internet to greater risks. Hence, understanding the factors that might affect the practice of secure behavior on smartphone networks by users, might lead information security professionals to design a better security systems for smartphones. In order to find some of the main factors that might affect security behavior practices, this study will use some of the theoretical frameworks that have been used to examine other human behavior. The theory of Planned Behavior (TPB; Ajzen, 1991), Theory of Reasoned Action (TRA; Ajzen & Fishbein, 1980), Theory of Protection Motivation (TPM; Rogers, 1975), and the Decomposition Theory of Planned Behavior (DTPB; Taylor & Todd, 1995c) have been widely used in the information security domain to find out what drives users to take proper security measures, what motivates users to use security technologies, or what motivates users to follow organizations' security policies (Herath & Rao, 2009). Finally, this study will derive a research model that is compatible with previous human behavioral theoretical frameworks and provide the foundation to formulate the model's hypotheses. The results of this study could be used by businesses' information-security specialists or other investigators in the domain of information security to provide and design a more robust and secure network that could provide higher degree of confidentiality, integrity, and availability of information security on smartphone networks.

### **Statement of the Problem**

There is insufficient data regarding the relationship between users' attitudes, intentions, perceived behavioral controls, and practicing security behaviors in the domain of

smartphone networks. This research attempts to fill that gap and expand our knowledge in this domain.

### **Objectives of the Research**

Due to the exponential growth of smartphone usage in personal and professional environments as one of the main devices that connects users to the Internet and business networks, there has been a great security concern among information-security specialists. Smartphone security has been shown to be problematic and inadequate (Androulidakis & Kandus, 2011b). Users of smartphones are the key players in providing security in smartphones and they must learn to value, and then practice, security behaviors to ensure the effectiveness of information security technologies and reduce the risk of security breaches.

One of the main objectives of this study is to examine the factors that affect users' behaviors toward the practice of security behavior on smartphones. This study is utilizing the Decomposed Theory of Planned Behavior (DTPB), which is based on TPB, as a core theoretical framework. The TPB identifies *intention* as a strong predictor of human behaviors—a construct believed to be applicable to security behavior in the use of information systems. Intention is postulated to be affected by attitude, subjective norms, and perceived behavioral controls. This research attempts to formulate a research model based on the DTPB to measure the effects of possible factors that might predict users' practice of security behaviors on their smartphones. This study will contribute to the expansion of previous research in the domain of smartphone security.

Since there are no established instruments available to assess the theoretical factors and their relationship to users' practice of security behaviors on their smartphones, the secondary objective for this study is to examine the psychometric properties (reliability and

validity) of the investigator-developed online-delivered survey questionnaire to be sure that one can have confidence in the study's outcomes.

The outcomes of this study might help other investigators in the area of information security to focus on human behaviors in the smartphone networks and design a more robust system that would ensure and enhance the three main goals of confidentiality, integrity, and availability of information security in smartphone networks. The results of this study might be utilized by organizations' information security experts to design information systems that are less vulnerable human incompetence with smartphone usages.

### **Proposed Model**

To find the factors that might affect users' security practice behaviors and derive the study's model, this paper must explain the relationship between *attitude*, *intention*, *behavioral control*, and outcome of *security practice behavior*. These four constructs were selected based on the social behavioral theories, TPB and DTPB, to form its research model.

**Behavior, behavioral control, intention, and attitude.** Smartphone security practice behaviors must be investigated from two dimensions. The first dimension is the recognition of the importance of adopting and using security technologies (e.g. antivirus/antispyware software). The second dimension is the actual use of security practices (e.g., choosing strong passwords, regular backing up of data, exercising caution with suspicious email attachments, and updating firmware). Ajzen states that "A central factor in the theory of planned behavior is the individual's intention to perform a given behavior. Intentions are assumed to capture the motivational factors that influence a behavior; they are indications of how hard people are willing to try or of how much of an effort they are planning to exert, in order to perform a given behavior. As a general rule, the stronger the intention to engage in a behavior, the more

likely should be its performance” (Ajzen, 1991, p. 181).

According to TPB, users’ behavior can be predicted by their intentions (Ajzen, 1988) and behavioral intentions could be predicted with high degree of accuracy by attitude toward the behavior, subjective norms, and perceived behavioral control (Ajzen, 1991).

“The Theory of Planned Behavior along with the Theory of Reasoned Action, which posits that intentions are based on attitudes and subjective norms, provides the basis for an examination of the relationship between attitude, intention, and behavior” (Herath and Rao, 2009, p. 108). The Theory of Planned Behavior (TPB) has been used widely in the information system domain and has been validated in studies with topics including: intention toward Internet abuse (Galletta & Ploak, 2003) and adaptation of E-commerce (Pavlou & Fygenon, 2006).

The Decomposed Theory of Planned Behavior (DTPB) is derived from TPB and the Technology Acceptance Model, and meant to provide better insight into the relationship between attitude, intention, and behavior. The derivation of the DTPB has been used in multiple studies of information security systems to measure the intention of the users to engage in the practice of security behavior. For instance, Ng and Rahim (2005) used DTPB to identify the user’s intentions and attitudes toward practicing security on home computers. In the present study, intention is modeled by constructs of perceived usefulness, perceived ease of use, and compatibility; subjective norm formed by peer influence, influence of respected people, and media influence; perceived facilitation condition modeled by self-efficacy, resource facilitation condition, and technology facilitating conditions. This research utilizes the DTPB as a core theoretical framework and expands the theory by identifying

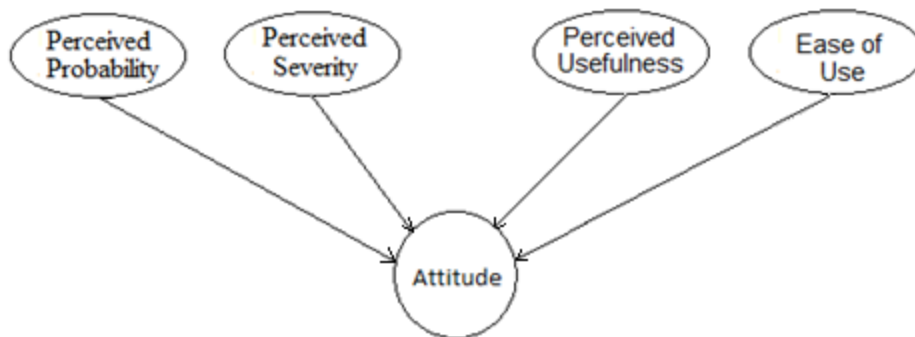
other factors that may affect users' attitudes towards practicing security behaviors in smartphone networks.

**Attitude.** Attitude is a good predictor of human intention and behavior (Kutluca, 2011). According to the TPB, users' responses toward a behavior or technology as a result of their intention, this can be predicted quite accurately by looking at users' attitude toward the behavior, subjective norms, and perceived behavioral control (Ajzen, 1988, 1991). Since intention and then behavior could be predicted through users' attitude toward a behavior, it is vitally important to identify the main factors that have an effect on users' attitudes towards practicing security behavior.

*Attitude* is a "...psychological tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor" (Eagly & Chaiken, 1993; Ferguson & Bargh, 2007]). Attitude defined as, "...a learned predispositions to respond positively or negatively to a specific object, situation, institution, or person" (Aiken, 2000 [as cited in Yushau, 2006]). According to the Technology Acceptance Model (TAM), attitude could be affected by two factors of, "...perceived usefulness and perceived ease of use" (Davis, 1989). Using DTPB in studying information technology usage, Taylor and Todd (1995c) combined TPB and TAM and suggest that attitude could be affected by compatibility.

Moreover, according to Anderson and Agarwal (2010), "The greater and more relevant the threat appears to be, the more likely the individual is to have a positive attitude about taking action. This positive attitude results in stronger intentions to act (Rogers, 1975) and lower likelihood that the individual will ignore security behavior" (p. 622). Fear appeals (Witte & Allen, 2000) and Protection Motivation Theory (PMT) "...identifies that the motivation to protect depends upon three factors: (1) perceived severity of a threat; (2)

perceived probability of the occurrence, or vulnerability; and (3) the efficacy of the recommended preventive behavior (the perceived response efficacy)” (Roger, 1983 [as cited in Herath and Rao, 2009, p. 109]). In other words, if the users perceive that the probability of security breaches on their smartphone is high (“perceived security of breaches”), any security breaches could risk their resources (“perceived severity of a threat”), and they believe the security practice behaviors on their smartphone can be effective (“perceived efficacy of recommended behavior”), they will adopt the preventive actions, which in the smartphone domain means using security technologies and security behavior. Previous theoretical models related to the factors that affect attitude lead us to the model that is presented in Figure 1.



*Figure 1.* Factors that affect attitude

Considering the DTPB and the factors that are posited to affect users’ attitudes toward smartphone security practices, this study proposes the research model illustrated in Figure 2 including the central constructs of *intention*, *attitude*, *behavioral control*, and *behavior* as they relate to smartphone security. Figure 2 also includes two additional variables, *computing experience* and *information security breach experience*, which might affect users’ information security behavior. It is predicted that if the users have more computing and security breach experiences and information security knowledge, then they

are more inclined to adopt more robust information security technologies and engage in more security behaviors.

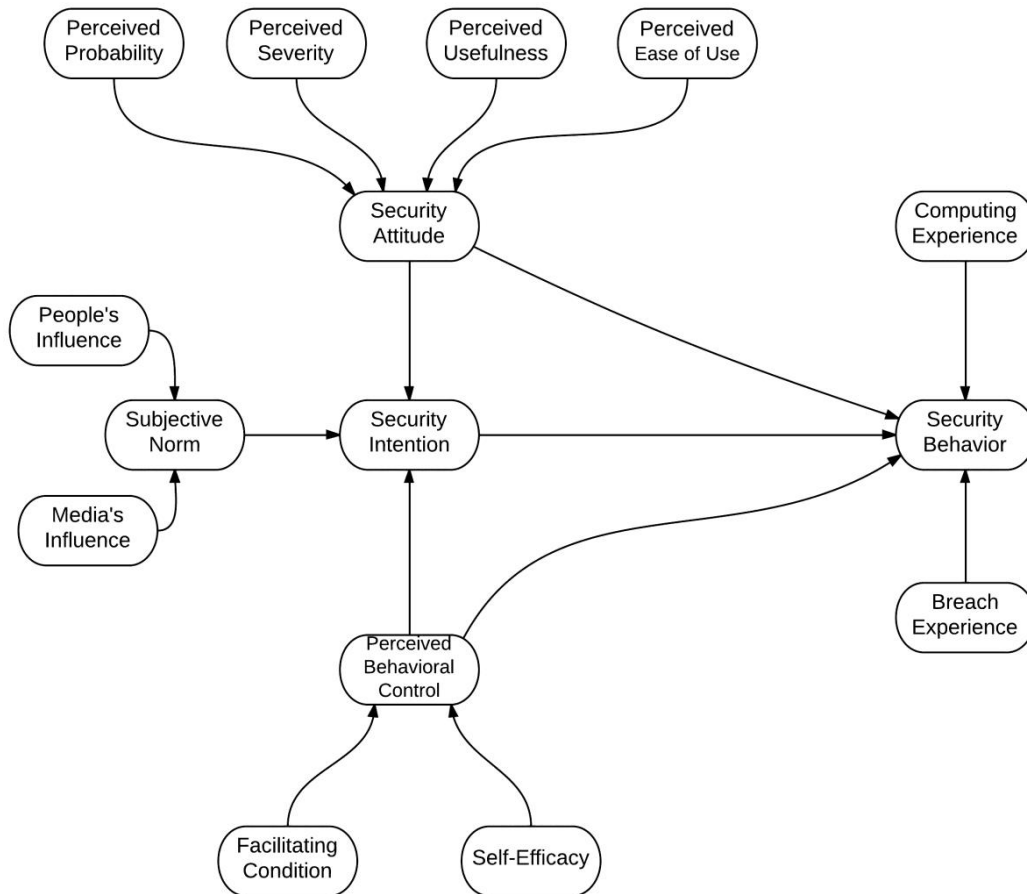


Figure 2. Proposed Research Model

**Research questions.** Based on the proposed research model, this study is designed to answer the following questions:

In the domain of smartphone networks,

1. What are the factors that might affect users' attitudes toward practicing security behaviors in the domain of smartphone networks?
2. What are the factors that might affect users' subjective norms on users'-in smartphone networks?



3. What are the factors that might affect users' perceived behavioral control?
4. What are the factors that might affect users' intentions toward practicing- security behaviors in smartphones?
5. What are the factors that might affect users' practicing security behaviors in smartphones?

**Research hypotheses.** According to the theoretical framework and the proposed research model, this study will test the hypotheses shown in Figure 3 and listed below.

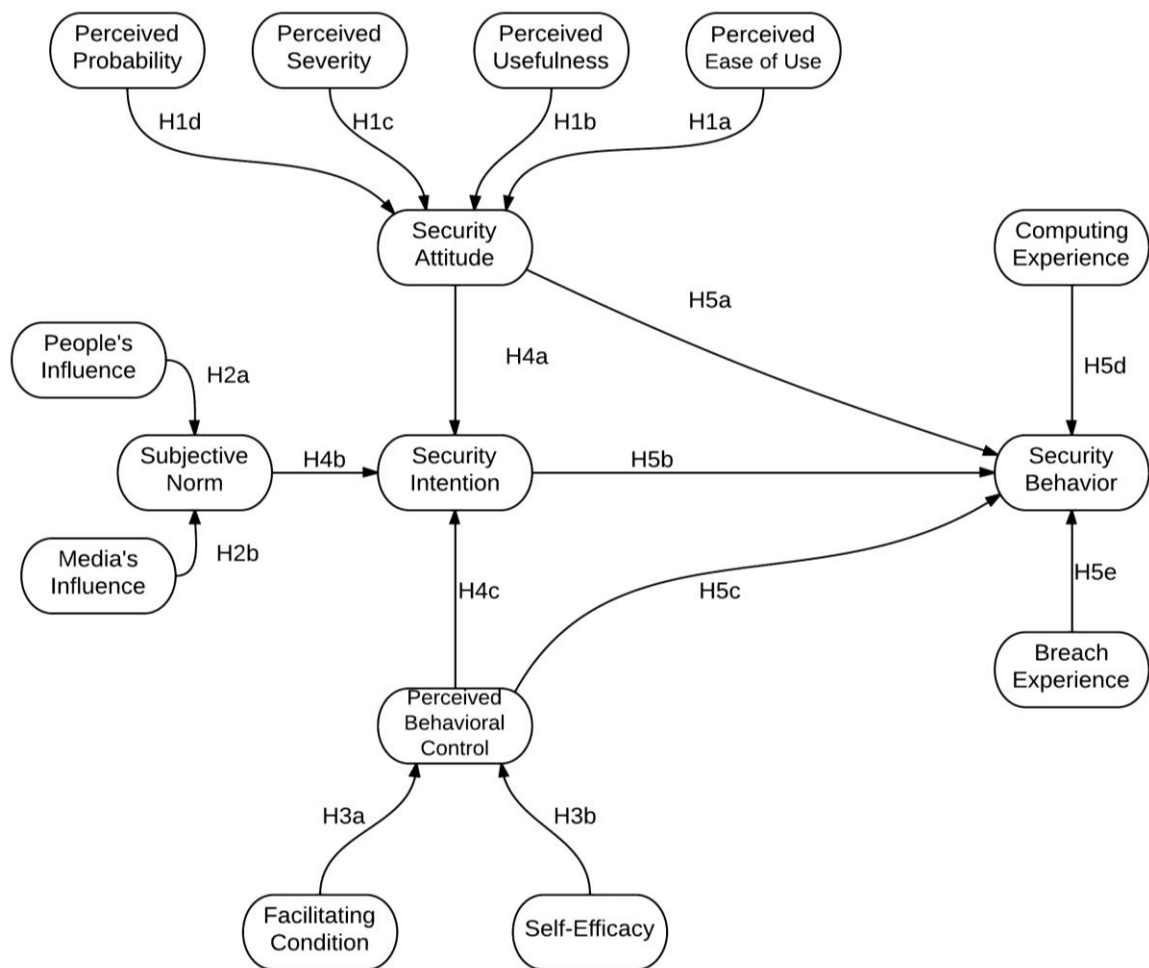


Figure 3. Research Hypotheses

H1a. There is a positive relationship between users' perceived ease of use of and the attitude to practice security behavior in smartphones.

H1b. There is a positive relationship between users' perceived usefulness and attitude to practice security behavior in smartphones.

H1c. There is a positive relationship between users' perceived severity of security breaches and attitude to practice security behavior in smartphones.

H1d. There is a positive relationship between users' perceived probability of security breaches and attitude to practice security behavior in smartphones.

H2a. There is a positive relationship between users' people's influence and subjective norm to practice security behavior in smartphones.

H2b. There is a positive relationship between users' media's influence and subjective norm to practice security behavior in smartphones.

H3a. There is a positive relationship between users' facilitating conditions and perceived behavioral control to practice security behavior in smartphones.

H3b. There is a positive relationship between users' self-efficacy and perceived behavioral control to practice security behavior in smartphones.

H4a. There is a positive relationship between users' attitude and intention to practice security behavior in smartphones.

H4b. There is a positive relationship between users' subjective norm and intention to practice security behavior in smartphones.

H4c. There is a positive relationship between users' perceived behavioral control and intention to practice security behavior in smartphones.

H5a. There is a positive relationship between users' attitude and practicing security behavior in smartphones.

H5b. There is a positive relationship between users' intention and practicing security behavior in smartphones.

H5c. There is a positive relationship between users' perceived behavioral control and practicing security behavior in smartphones.

H5d. There is a positive relationship between users' computing experience and practicing security behavior in smartphones.

H5e. There is a positive relationship between users' information security breach experience and practicing security behavior in smartphones; the more breach experience, the higher the level of security behaviors in smartphones.

**Limitations.** The smartphone network system is made of firmware, software, hardware, and users. This study will focus solely on users and does not focus on firmware, hardware, or software. This research will focus on the smartphone users who utilize the devices to connect to the Internet or business networks. Smartphone security practice behavior here will be limited to the adoption of security technologies (e.g., antivirus/antispyware, password, and getting backup) and security behavior (i.e., using strong password, backing up files/data, using antivirus/antispyware, and carry out these security behaviors on a regular schedule).

**Assumptions.** The first assumption is that the users will respond to the survey without any bias. The sampling pool available, however, was primarily students who, as a group, may not be representative of the broader population of smartphone users. The second assumption is that the investigator-designed survey questionnaire will demonstrate adequate

validity and reliability to have confidence in the outcomes of the analyses.

**Definitions of terms.** *Attitude* is "... a psychological tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor" (Eagly & Chaiken, 1993; Ferguson & Bargh, 2007).

*Breach Experience* (BE) is defined as users' previous information security incidents, such as getting viruses, spyware, smartphone loss, and/or data loss.

*Computing Experience* (CE) has been defined as the computing experience as the users' knowledge and experience in the computers, Internet, and information security (Kim & Ryu, 2009).

*Information security* "...refers to the protection of information and the systems that use, store, and transmit information (Whitman & Mattord, 2011). The three key attributes of information security are confidentiality, integrity, and availability (Smith, 1989 [as cited in Rhee, Kim & Ryu, 2009], p. 818).

*Intention* can be defined as behavioral intentions which can be predicted with high degree of accuracy by attitude toward the behavior, subjective norms, and perceived behavioral control (Ajzen, 1991).

*Information security threats* are, "Security incidents that may compromise an asset, resulting in undesirable action" (Summers, 1997 [as cited in Clark, 2011]).

*Information Security Practice*: "Individuals' information security risk management behavior involving two aspects: the adoption of security technology and security conscious care behavior related to computer and Internet usage. The former is related to the use of security software and features such as Anti-virus software, Anti-spyware, and a pop-up blocking function. The latter refers to security compliance behavior in using a computer and

the Internet, such as use of a strong password and frequency of making a back-up copy” (Rhee, Kim & Ryu, 2009, p. 818).

*Smartphone information security practices* include two behaviors. First, the adoption and usage of security technologies such as antivirus, antispyware, encryption, and second, robust security behaviors such as: selecting strong passwords, updating security patches, and making backups.

*Smartphone network* implies a network that enables smartphones to connect to the Internet and share their resources with others.

*Subjective norm*: “This refers to a person’s perception of the social pressure to perform or not to perform the behavior under consideration” (Ng & Rahim, 2005).

*Perceived Behavioral Control* “...reflects beliefs regarding access to the resources and opportunities needed to perform a behavior” (Taylor & Todd, 1995b, p. 139).

*Perceived Usefulness* is defined as users’ belief that adaptation of a certain behavior is useful and will enhance performance (Taylor & Todd).

*Self-efficacy* defined as “People’s judgments of their capabilities to organize and execute courses of action required attaining designated types of performances” (Bandura, 1986, p. 391).

*Self-efficacy in information security* (SEIS) is defined as “A belief in one’s capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability” (Rhee, Kim & Ryu, 2009, p. 818).

*Smartphone Information Security Self-Efficacy* is individual judgment of a person’s ability to practice information security behavior on smartphone networks.

*Technology Behavior Control (TBP)*: According to TPB, users' behavior can be predicted by their intention (Ajzen 1988) and behavioral intentions could be predicted with high degree of accuracy by attitude toward given behavior, subjective norms, and perceived behavioral control (Ajzen, 1991).

### **Summary**

The first chapter is an introduction to the research, including the statement of the problem, the purpose and significance of this study, the research scope, and research objectives. It also identifies a number of recognized theories relevant to the goal of identifying the factors that might affect users' behavior toward practicing security behaviors on smartphones. Finally, it presents the proposed research conceptual model and hypotheses. In the following chapter, the relevant literature is more thoroughly reviewed.

## **Chapter 2. Review of the Literature and Background**

### **Introduction**

Because this study is going to examine the factors that affect users' information security behavior on smartphones, it will heavily focus on literature related to the different methods of measuring information security behaviors. Moreover, it will focus on the theoretical frameworks that have been used to predict users' behavior on different domains such as computer security and information security.

### **Smartphone Security**

Lazou and Weir (2011) state that, "Mobile devices are by nature more vulnerable to theft and accidental loss than larger systems in fixed locations" (p. 183). As a result, providing security for mobile networks and avoiding information breaches are some of the main daily challenges of Information System Security specialists in smartphone networks. Not only can an unsecured smartphone device risk the security of personal data, but it could also risk business' information assets. Therefore, employees who use their personal smartphones at work pose more risk to a company's information security (Egan et al., 2012). "Users create an open back door into our corporate networks through their Internet-enabled services, third-party application use, and electronic interaction (i.e. email) with other users. This vulnerability is increased when mobile systems that join home and other commercial networks" (Dodge, Carver, & Ferguson, 2007, p. 73).

Utilizing robust security technologies such as strong passwords, encryption, antivirus, firewalls, and anti-spyware could reduce the risk of security breaches on smartphone networks, if users show enough interest to learn and utilize them. For example, smartphone networks would be unsecured and vulnerable to security breaches if users do not practice security behaviors. Not only can these vulnerable devices jeopardize confidentiality,

integrity, and availability of the individuals' sensitive data but they could jeopardize any public or private networks that they use to connect to Internet. In other words, users of smartphone devices play an important role in providing information security in smartphone networks, which affect the information security of private and public networks.

Although smartphone companies provide several security tools such as password encryption, firewalls, antivirus, and antispyware that could mitigate the risk of security breaches on smartphone networks, several research studies have shown that the users of smartphones fail to adopt these technologies. For instance, the empirical study of "Mobile Phone Security Awareness and Practices of Students in Budapest" by Androulidakis and Kandus (2011) showed that only 12.3 percent of the users actually employed antivirus software and only 24.5 percent of the respondents had passwords on their phones. Although there have been several studies that illustrated the requirement for information security on smartphones, few studies have focused on the adoptions of security behavior and security technologies from the users' points of view.

### **Theoretical Frameworks**

Ng, Kankanhalli, and Xu (2009) stated that the Technology Acceptance Model (TAM) and the Theory of Planned Behavior (TPB) can be applied to examining the intention to adopt and use computer security behavior such as use of security technologies.

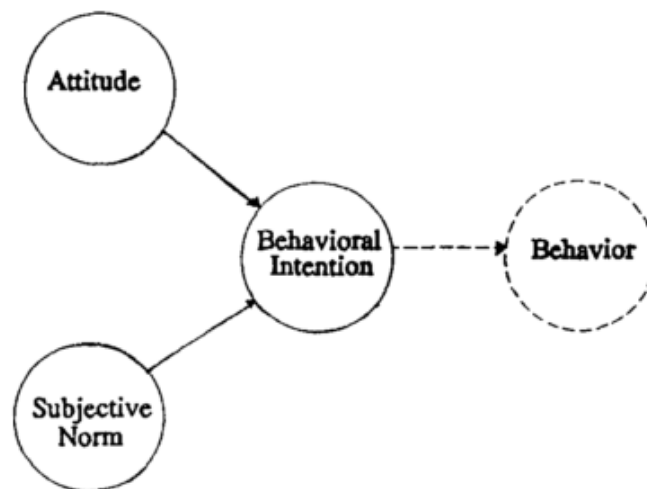
In another study by Taylor and Todd (1995c), the authors compare three theoretical frameworks of DTPB, TAM, and PMT to examine users' intentions to adopt Information Technology. They found that, "TAM explains 52% of the variance in behavioral intention while original TPB explains 57%, and decomposed TPB, 60% of the variance in intention" (p. 166).



For these reasons, this study involves an in-depth review of the literature and those theoretical frameworks that have been used to examine users' behavioral and technological adaptation of security practices. Finally, this study will derive a theoretical model that will be used to find more information about the users' behaviors toward smartphone security.

Understanding the factors that might affect the practice of secure behavior on smartphone networks by users might lead researchers in the area of information security to design better security systems for smartphones. In order to find some of the main factors that might affect users' practice of security behavior on smartphone networks; this study will use some of the theoretical frameworks that have been used to examine human behavior.

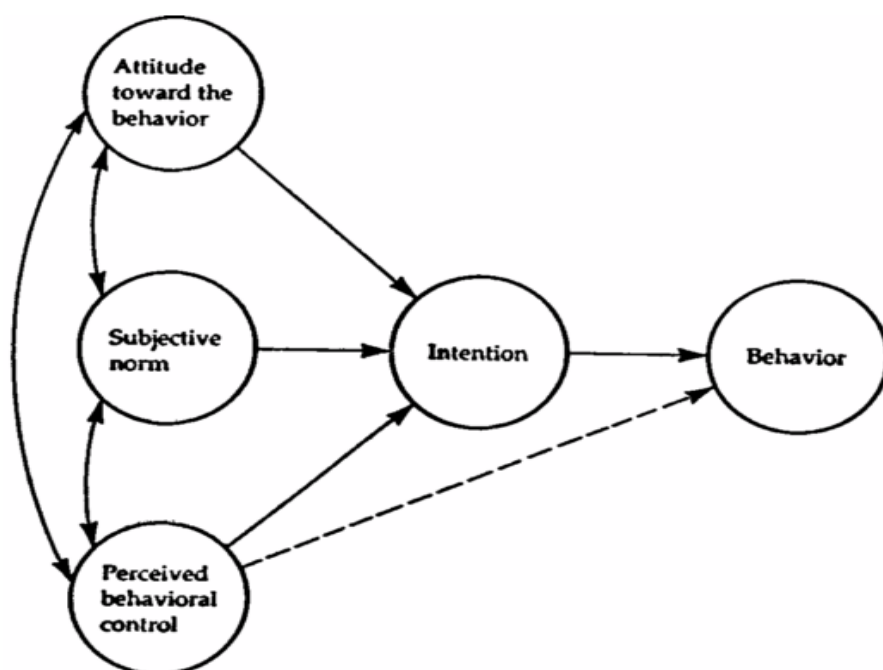
**Theory of planned behavior.** According to the Theory of Reasoned Action (TRA), illustrated in Figure 4, Behavior is affected directly by Behavioral Intention, and Behavioral Intention is modeled as a function of Attitude and Subjective Norm (Fishbein & Ajzen, 1975).



*Figure 4.* Theory of Reasoned Action (Fishbein & Ajzen, 1975)

The Theory of Planned Behavior (TPB; Ajzen, 1988, 1991) introduced another factor that impacts behavioral intention, that is, Perceived Behavioral Control (PBC), to improve

the Theory of Reasoned Action (TRA). According to the authors, PBC, "...reflects beliefs regarding access to the resources and opportunities needed to perform a behavior" and will affect Behavioral Intention and Behavior as shown in Figure 5 (Taylor & Todd, 1995b, p. 139). Ajzen (1991) states that the TPB, "...incorporates some of the central concepts in the social and behavioral sciences, and it defines these concepts in a way that permits prediction and understanding of particular behaviors in specified contexts" (p. 206).



*Figure 5.* Theory of Planned Behavior (Ajzen, 1991, p. 182)

According to the TPB, individuals' behavior is affected by motivation (intention) and their ability (behavioral control) and has a direct relationship with performing a specific behavior. "Intentions are assumed to capture the motivational factors that influence a behavior; they are indications of how hard people are willing to try, of how much of an effort they are planning to exert, in order to perform the behavior. As a general rule, the stronger the intention to engage in a behavior, the more likely should be its performance" (p. 181).

For instance, if an individual illustrates a strong intention toward practicing information security technologies and has the required means and ability, it is more likely that he/she would perform the behavior. In other words, the TPB highlights the impact of intention and behavioral control on behavior and states that users' behavior can be predicted by their intention. Moreover, as illustrated in Figure 5, the Theory of Planned Behavior identifies three main factors of attitude toward the behavior, subjective norms, and perceived behavioral control as the main factors that impact behavioral intention (Ajzen, 1988, 1991). "The theory of planned behavior postulates three conceptually independent determinants of intention. The first is the attitude toward the behavior and refers to the degree to which a person has a favorable or unfavorable evaluation or appraisal of the behavior in question. The second predictor is a social factor termed subjective norm; it refers to the perceived social pressure to perform or not to perform the behavior. The third antecedent of intention is the degree of perceived behavioral control which, as we saw earlier, refers to the perceived ease or difficulty of performing the behavior and it is assumed to reflect past experience as well as anticipated impediments and obstacles. As a general rule, the more favorable the attitude and subjective norm with respect to a behavior, and the greater the perceived behavioral control, the stronger should be an individual's intention to perform the behavior under consideration" (Ajzen, 1991, p. 188).

**Technology acceptance model.** Another theoretical frame work that could help us to understand the users' acceptance or rejection of technology or a related action is the Technology Acceptance Model (Davis, 1989, 1993; Davis, Bagozzi, & Warshaw, 1989), which is presented in Figure 6. TAM, which is an adaptation of TRA (Fishbein & Ajzen, 1975), states that two beliefs of perceived usefulness and perceived ease of use are the main

determinants of an individuals' intention to adopt or not adopt a particular technology (Taylor & Todd, 1995c).

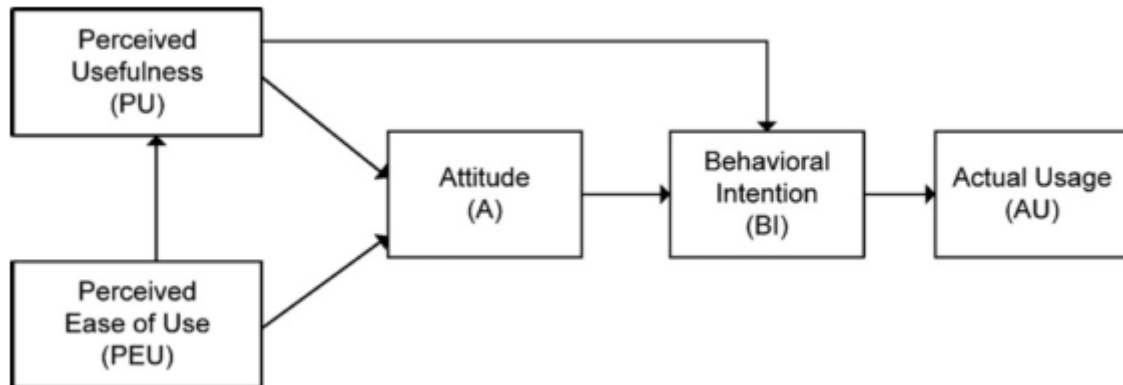
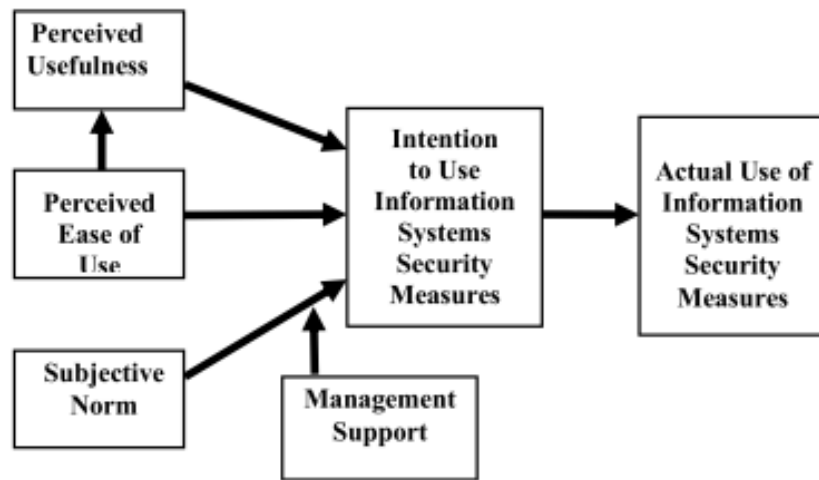


Figure 6. The Technology Acceptance Model (Taylor & Todd, 1995c)

TAM models actual usage as a direct function of behavioral intention and the behavioral intention as a function of attitude and perceived usefulness. The author suggested that the perceived usefulness might have direct relationship with behavioral intention, which represents the favorable or unfavorable feelings of individuals towards using the technology. Moreover, the perceived usefulness reflects the belief that using the technology will enhance performance, which will be determined by ease of use. In other words, if an individual feels that performing a task is easy, it is more likely that he/she would find that technology beneficial and lead to the adoption of that technology. For instance in this study, the TAM could shed light on the impact of Perceived Usefulness and Ease of Use on individuals' attitude toward adaptation of the security technologies.

In the study of TAM and "Employees Adaptation of Information Systems Security Measures" by Jones, McCarthy, Halawi, and Mujtaba (2010), hypotheses were based on the model presented in Figure 7 and derived from TAM. The authors didn't use attitude as a

mediator of intention and hypothesized that the perceived usefulness and perceived ease use would affect intention.



*Figure 7.* TAM and information system security adaptation (Jones, McCarthy, Halawi & Mujtaba, 2010)

The results of the study, however, rejected their hypotheses about Perceived Usefulness and Perceived Ease of Use and showed that these factors were not found to have a strong effect on intention to use computer information security measures. For instance, in the study performed by Taylor and Todd (1995c) about IT usage, the authors found a positive relationship between perceived usefulness and intention, and perceived usefulness and ease of use had positive relationships with attitude. Moreover, the study supported the previous finding about the positive relationship between perceived ease of use and perceived usefulness. Also, the study found subjective norm and management support to have a strong effect on intention to use the computer information systems security measures. However, the authors did not actually test the relationship between intention to use information systems security measures and actual use. For future studies, the authors recommended considering

the given attributes and using the Theory of Planned Behavior to examine the users' information systems security adaptation.

In a study performed by Kim (2008), the author tested the adoption of a smartphones and defined the intention of using the devices as a function of Perceived Ease of Use and Perceived Usefulness. The study found positive relationships between the two factors as well as between each of the factors and Intention.

Perceived Usefulness and Perceived Ease of Use identified by TAM as two more perception factors that can impact users' technological adaptation behavior, have been supported by most of the research reported. They, therefore, will be utilized by this study to examine the factors that impact attitudes toward using information security technology in smartphones.

**Decomposed theory of planned behavior.** Taylor and Todd (1995a, 1995b, 1995c), in order to better explain the people's intention to adopt behavior, decomposed the TPB and introduced the Decomposed Theory of Planned Behavior (DTPB). The authors state that, "Each of the determinants of Intention, i.e., Attitude, Subjective Norm, and Perceived Behavioral Control, is, in turn, determined by underlying belief structures..." as it is shown in Figure 8.

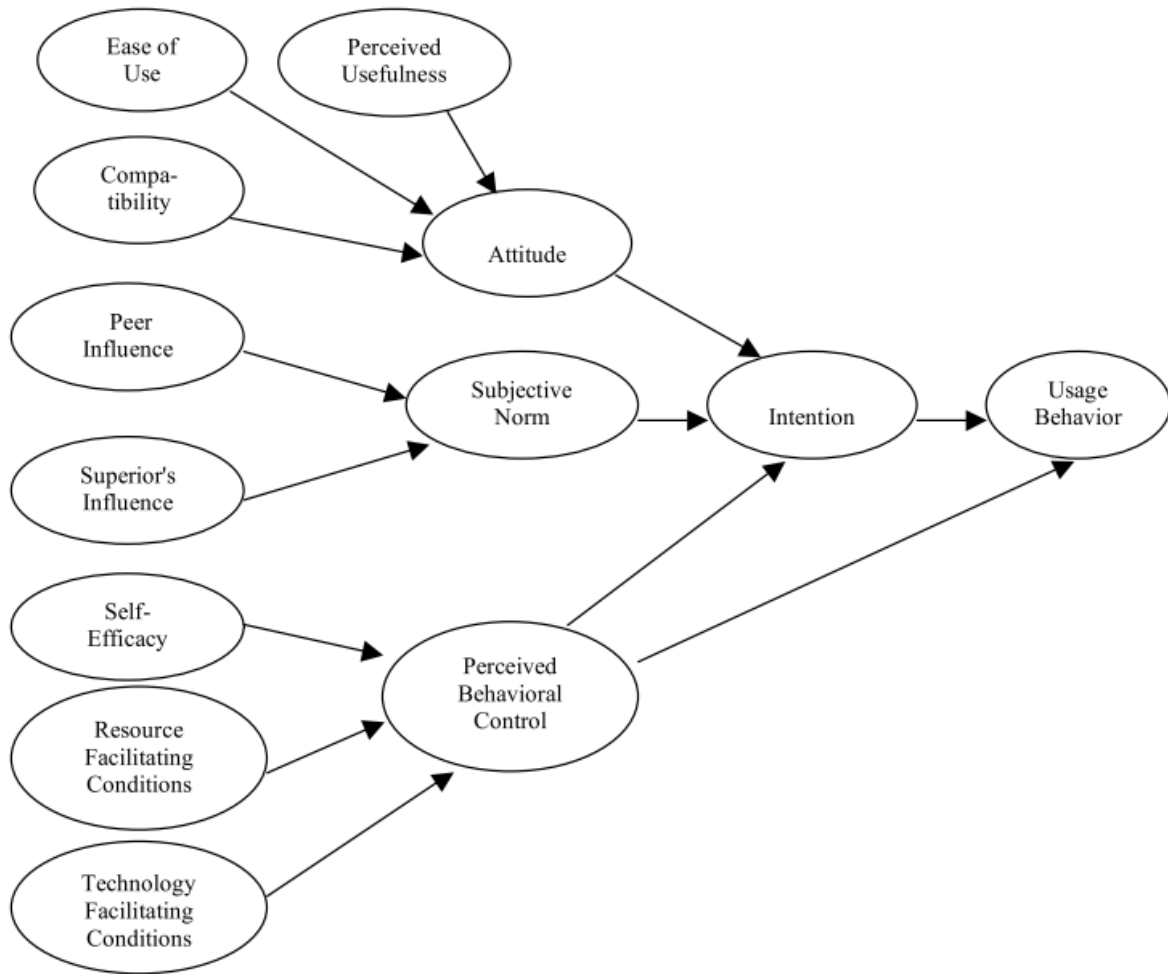


Figure 8. Decomposed Theory of Planned Behavior (Taylor & Todd, 1995c)

According to the DTPB model, Attitude, Subjective Norm, and Perceived Behavioral Control are constructed as following:

(1) Attitude is modeled as a function of Perceived Usefulness (relative advantages), Ease of Use (Complexity), and Compatibility.

(a) Perceived Usefulness refers to the degree to which a person believes that certain behavior could be beneficial and accompanied by advantages such as economic benefits, image enhancement, convenience, and satisfaction (Rogers, 1983 [as cited in Taylor & Todd, 1995b]). According to DTPB, relative advantages or

“Perceived Usefulness,” will affect attitude directly and eventually act as a motivational factor (intention) for that individual to perform a particular task.

Davis (1989 [as cited in Yuen, 2004, p. 238]) defines Perceived Usefulness as,

“...the degree to which a person believes that using a particular system would enhance his job performance.”

(b) Ease of use refers to the individual’s belief regarding the degree of ease or difficulty required to perform a task. According to this theory, if someone believes that performing a particular task is difficult, it less likely that he/she will perform that task.

(c) “Compatibility is the degree to which the innovation fits with the potential adopter's existing values, previous experiences, and current needs. In general, as the perceived relative advantages and compatibility of information technology usage increase, and as complexity decreases, attitude towards information systems usage should become more positive” (Rogers, 1983 [as cited in Taylor & Todd, 1995c, p. 152]).

(2) Subjective norm is modeled as a function of internal and external normative influences.

According to this factor, an individual’s behavior can be influenced by other individuals.

(a) There are three main groups of people that could impact individuals’ behavior, i.e., superiors, peers, and subordinates. In other words, according to the concept of subjective norms, individuals might be inclined to perform or avoid a behavior as a result of their supervisors, peers, or subordinates either performing or avoiding it. For instance, Taylor and Todd (1995c) identify two of these groups, i.e., other students (peers) and professors (superiors) as people that affect students’ intentions toward usage of Information Systems.



(b) In another study related to the adoption of security behavior in personal computers, Yuen (2004) identified mass media, as well as family and peers as main constructs that affect subjective norms.

(3) Perceived Behavioral Control is modeled as a function of self-efficacy, resource-facilitating conditions, and technology-facilitating conditions.

(a) Self-efficacy is an individual's belief or perceived ability to perform a particular action. For instance, if an individual believes that he/she has the ability to perform a desired behavior, then it is more likely that he/she will perform that action.

(b) The resource-facilitation condition factor measures the impact of resource availability to perform a behavior. For example, Taylor & Todd (1995c) identified time and money as facilitation resources that could affect the individual's intention toward utilizing information technology (IT).

(c) The technology-facilitation condition factor assesses the availability of technological resources to perform a behavior, and is modeled as an additional factor that could impact the perceived behavioral control and intention, which is thought to lead to the adoption of a behavior.

The DTPB has been widely used to predict human behavior toward adaptation of particular actions. Among the topics studied are "customer adaptation intention" (Taylor & Todd, 1995b); "household recycling and composting intentions" (Taylor & Todd, 1995a); "Information technology usage" (Taylor & Todd, 1995c); and "home computer users' intention to practice security" (Yuen, 2004). In the report, "a socio-behavioral study of home computer users' intention to practice security" by Yuen (2004), the author utilized a model (see Fig. 9) that has been derived from DTPB to measure the influence of the factors that

impact the home users' intention toward practicing security behavior. The author Subjective norm is modeled as a function of internal and external normative influences. According to this factor, an individual's behavior can be influenced by other individuals.

There are three main groups of people that could impact individuals' behavior, i.e., superiors, peers, and subordinates. In other words, according to the concept of subjective norms, individuals might be inclined to perform or avoid a behavior as a result of their supervisors, peers, or subordinates either performing or avoiding it. For instance, Taylor and Todd (1995c) identify two of these groups, i.e., other students (peers) and professors (superiors) as people that affect students' intentions toward usage of Information Systems.

In another study related to the adoption of security behavior in personal computers, Yuen (2004) identified mass media, as well as family and peers as two main constructs that form subjective norms.

Perceived Behavioral Control is modeled as a function of self-efficacy, resource-facilitating conditions.

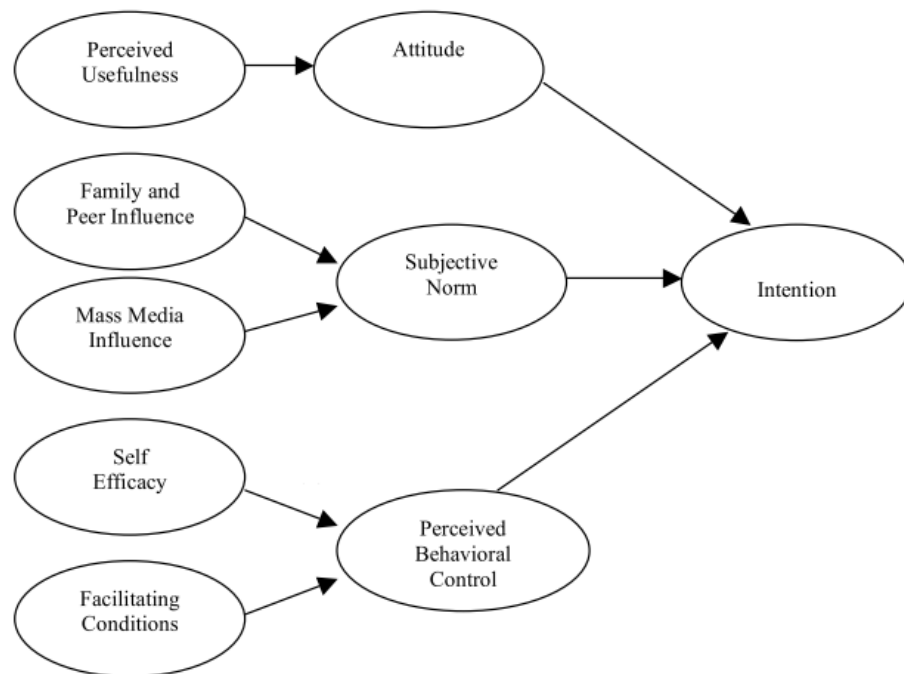
Self-efficacy is an individual's belief or perceived ability to perform a particular action. For instance, if an individual believes that he/she has the ability to perform a desired behavior, then it is more likely that he/she will perform that action.

The resource-facilitation condition factor measures the impact of resource availability to perform a behavior. For example, Taylor & Todd (1995c) identified time and money as facilitation resources that could affect the individual's intention toward utilizing information technology (IT).

The technology-facilitation condition factor assesses the availability of technological resources to perform a behavior, and is modeled as an additional factor that could impact the

perceived behavioral control and intention, which is thought to lead to the adoption of a behavior.

The DTPB has been widely used to predict human behavior toward adaptation of particular actions. Among the topics studied are “customer adaptation intention” (Taylor & Todd, 1995b); “household recycling and composting intentions” (Taylor & Todd, 1995a); “information technology usage” (Taylor & Todd, 1995c); and “home computer users’ intention to practice security” (Yuen, 2004). In the report, “a socio-behavioral study of home computer users’ intention to practice security” by Yuen (2004), the author utilized a model (see Figure 9) that has been derived from DTPB to measure the influence of the factors that impact the home users’ intention toward practicing security behavior.



*Figure 9.* Model of home users' intention to practice computer security (Yuen, 2004)

The author measures the users’ intention to practice security behavior by investigating their intentions toward specific behaviors such as updating their computers’ antivirus

program; backing up their critical data; and using a personal firewall. Finally, the research shows that attitude and subjective norm have significant positive relationships with intention to practice all security behaviors while perceived behavioral control is a significant predictor only of intention to use a firewall. Moreover, perceived usefulness has significant positive relationship with attitude; family and peers and mass media influences have significant positive relationship with subjective norm; and although self-efficacy has a significant positive relationship with perceived behavioral control, the study reported no significant relationship between facilitating condition and perceived behavioral control.

Due to the fact DTPB has been used widely in intention and behavioral prediction and has been validated widely by a number of studies (Taylor & Todd, 1995a, 1995b, 1995c, Yuen, 2004), it appears to be appropriate to use in the identification of the factors that influence users' information security behavior on smartphones. These theories could be used to identify the main factors that encourage users to adopt security behaviors and security technologies.

**Fear appeals and protection motivation model.** Individuals might adjust their behavior toward adoption of an action or a technology based on the degree of severity and cost of the damage that they may perceive that a particular threat might cause, which is known as *perceived severity of threat* (Grothmann & Reusswig, 2006, Pyszczynski, Greenberg, & Solomon, 1997). Workman, Bommer, and Straub (2008) posit that “Perceived severity of threat will lead people to behave in a more cautious manner if their perceptions of the damage or danger increase. The reverse of this, however, is also true: when people perceive that a risk has diminished, they will behave in a less cautious manner” (p. 2803).

Fear appeals (Witte & Allen, 2000) and Protection Motivation Theory (PMT; Roger, 1983), "...identifies that the motivation to protect depends upon three factors: (1) perceived severity of a threat; (2) perceived probability of the occurrence, or vulnerability; and (3) the efficacy of the recommended preventive behavior (the perceived response efficacy)" (Herath and Rao, 2009, p. 109).

According Anderson and Agarwal (2010), "The greater and more relevant the threat appears to be, the more likely the individual is to have a positive attitude about taking action. This positive attitude results in stronger intentions to act (Rogers, 1975) and lower likelihood that the individual will ignore security behavior" (p. 622).

PMT and fear appeals have been used widely in health care disciplines as well as the information security domain to predict users' behaviors. For instance, Woon, Tan, and Low (2005) used PMT to identify factors that make some wireless Internet users at home secure their networks while others, given the same factors, do not. The aim of the study was to test whether threat appraisal and coping appraisal played an important role in leading users to opt between either enabling or not enabling their wireless network security options. The result showed that perceived severity, response efficacy, and self-efficacy played a significant role in users' decisions about security options. The PMT model also has been used in predicting the likelihood of online users engaging in virus protection behaviors (Lee, Larose, & Rifon, 2008; Mahabi, 2010).

These studies examined the perceived severity of a threat and perceived probability of the occurrence as direct determinants of attitude, intention, and information security behavior adaptation. In other words, if individuals feel that the risk of not adopting a security behavior is high and/or the probability of falling into information security traps is very high, these

perceptions could affect users' attitude, intention and finally their behavior toward adaptation of information security technology or behavior. For instance, in the study of users' computer security behavior by Ng, Kankanhalli, and Xu (2009), the authors found that perceived susceptibility has a positive relationship with computer security behavior, but perceived severity does not. This study also found that perceived benefits and self-efficacy were the major determinants of the users' behavior. In a study by Workman, Bommer, and Straub (2008), it was shown that both perceived severity and perceived vulnerability have strong negative relationships with omission of information security behaviors. One of the recommendations of the authors for future studies was to include the perceived ease of use and perceived usefulness from TAM to better understand the users' behavior toward the adaptation of information systems security.

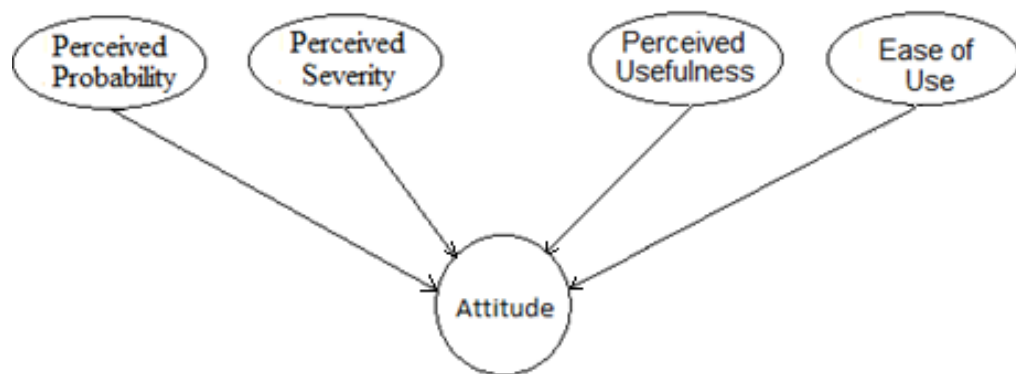
Not only have perceived severity threat and perceived threat of susceptibility from fear appeals and Protection Motivation theory been used by researchers for examining the intention and actual behavior in information security (Johnston & Warkentin, 2010; Workman, Bommer & Straub, 2008), but they also have been used to predict attitude as a determinant of intention and behavior. For example, Herath and Rao (2009) found that perceived *severity* of security breach will directly impact the security breach concern level among employees and then this security breach concern level can have a positive significant relationship with employees' attitude toward security policy compliance. On the contrary, the study did not find any significance between perceived *probability* of security breach and security breach concern level among employees.

In the context of information security in smartphones, if individuals sense an increased likelihood of security breaches on their devices and a higher severity of risks and damages as

a result of not adopting information security, then the concepts explored in the PMT and fear appeal literature can be applied to the context of information security. In other words, if the users perceive that the probability of security breaches on their smartphone is high (perceived probability of breaches), and any security breaches could risk their resources (perceived severity of a threat), and they believed the security practice behavior on their smartphone can be effective (perceived efficacy of recommended behavior), they will adopt the preventive actions, which in smartphone domain is using security technologies and security-insuring behaviors.

### **Information Security Adaptation Model**

Based on the fear appeals and PMT, attitude and intention could be modeled by perceived severity of a threat and perceived probability of the occurrence, or vulnerability. Moreover, TAM and DTPB modeled attitude as a function of perceived ease of use and perceived usefulness. For this reason, to better explain the attitude from individuals' perception this research adapts the following model as presented in Figure 10.



*Figure 10.* Security attitude and other latent variables

Finally the research model for this study is presented in Figure 11, which utilizes DTPB as a base and includes the perceived probability and perceived severity, which have been adapted from fear appeals and PMT.

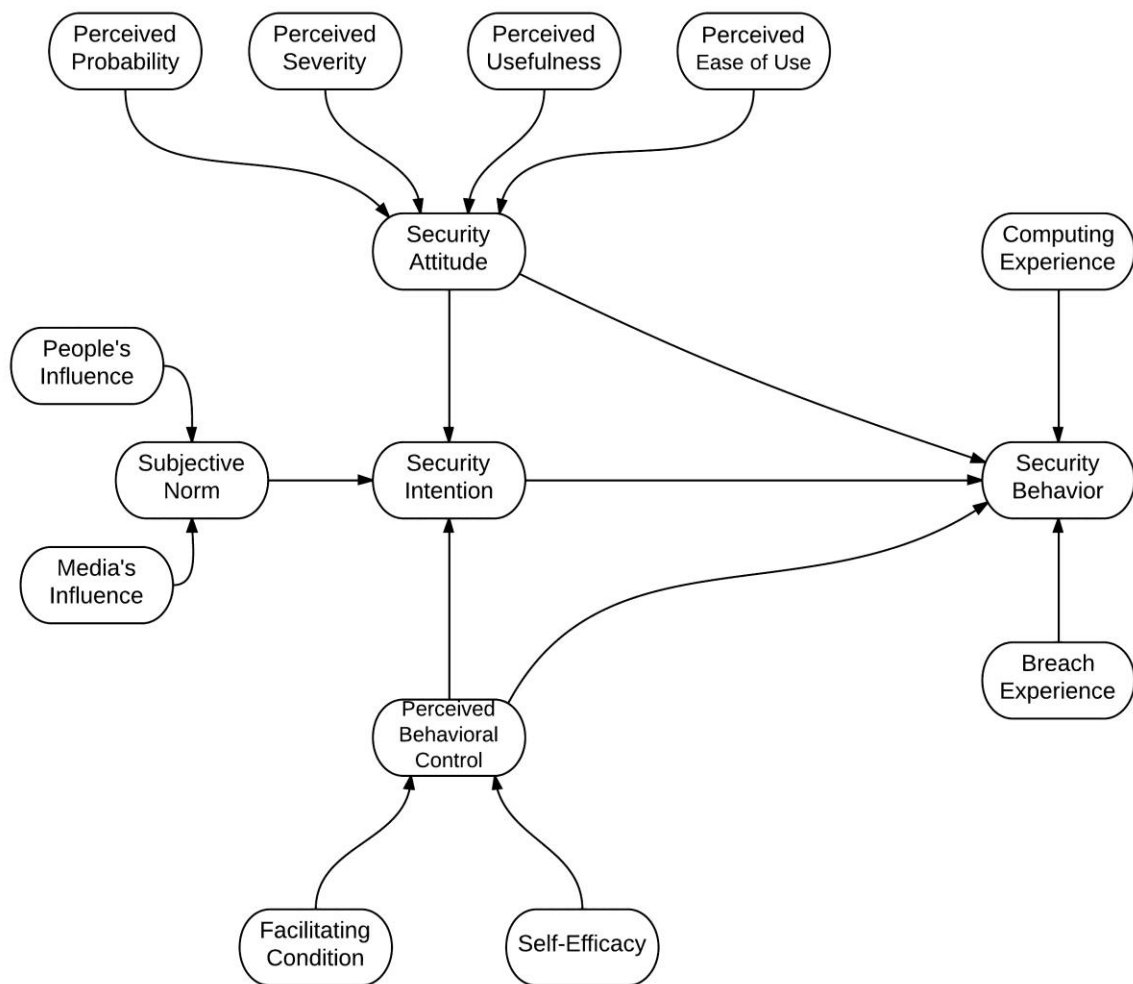


Figure 11. Smartphone information security behavior adaptation model

## Summary

Chapter 2 has provided background about information security behavior adoption by individuals. This chapter reviewed some of the literature and theoretical frameworks that have been used to examine human behavior toward adaption and utilization of a particular behavior or technology. Finally, by considering the literatures and considering the recommendation in the area of information security technology and behavioral adaption, this chapter introduced a theoretical model to examine the individuals' behavior toward utilizing



and adapting information security technology in smartphones. In Chapter Three, this study will provide more information about the research methodologies used to answer the research questions that have been generated based on the introduced research model.

## **Chapter 3. Research Methodology**

### **Introduction**

This chapter provides a detailed report of the research methodology that was utilized to test the theory-based research model of smartphone security behavior formulated in the second chapter. This chapter also discusses the specific steps of the research methods: population and sampling; instrumentation development and design; the pilot study; the psychometric properties (reliability and validity) and content of the scale; human subjects' considerations; data collection procedures; and the data analysis plan.

### **Research Methods**

This study was designed to examine theory-derived factors that could affect users' security behavior on smartphones such as: attitude, intention, perceived behavioral control, and subjective norms. The research model formulated in Chapter 2 was used to derive the research hypotheses. This research utilizes descriptive and correlational research methodology to examine its hypothesis. This methodology has been used extensively to test the relationships or correlations among multiple variables (Leedy & Ormrod, 2010) to predict a focal outcome. In the present study, the focal outcome is the security behavior of smartphone users.

### **Population and Sampling**

The target population for this research is all people who own or will own smartphones and who utilize it to connect to the Internet. Since students are one of the fastest growing groups of smartphone users, this study samples students at Eastern Michigan University. Although some students might not have a smartphone, they are most likely to have been exposed to information security technologies, e.g., passwords, antivirus/antispyware

programs, backup procedures, among others. Moreover, the responses from this sample of students could be used to compare two subgroups of respondents--those who own smartphones and those who do not. For this reason, convenience sampling was used to draw the subjects from among students at Eastern Michigan University. Moreover, to enlarge the sampling pool, this study used snowball sampling by encouraging respondents, which were mainly students, to identify and recruit other students whom they know to complete the survey.

### **Instrument Design**

This study utilized an investigator-developed online survey questionnaire to examine the research hypotheses and predictive research model formulated from the in-depth review of relevant theories and extant literature, reported in Chapter 2. The hypotheses derived from the model examined the factors that affect users' information security behavior with smartphones. The questionnaire in this survey collected data from items designed to measure constructs such as: perceived probability and perceived severity of risk/threat to smartphone security; perceived usefulness and perceived ease of use of smartphone security technologies; attitudes, subjective norms (defined as peer influence, supervisor /professor influence, and media influence) regarding use of smartphone security behavior; facilitating conditions, self-efficacy, perceived behavioral controls (perceptions of personal knowledge, ability and control to engage in security behavior); intention to engage in security behavior; and actual use of security behaviors. The study also collected some demographic data related to the users' age, gender, level of education, as well as relevant experience such as smartphone ownership, and Internet and smartphone computing experience, including experience with breaches of security. The first draft of the survey was derived from the literature and adopted

construct labels to fit the study of users' security behavior adoption for their smartphones. The first draft was presented to a panel of experts, made up of three tenure/track faculty members at Eastern Michigan University and three information security experts. The panel of experts ensured that the survey had good content validity. Each construct was measured through multiple items (questions) with each item measured utilizing a five-point Likert-type scale from 1, "strongly disagree" to 5, "strongly agree." As illustrated in Table 1, the items that have shown high levels of reliability and validity in previous studies have been selected to form this study's constructs.

Table 1

*Constructs and Items*

| <b>Construct</b> | <b>Items</b>   |
|------------------|--|
| Demographic      | Age<br>Gender<br>Education Level<br>Years of Education after high school<br>Major<br>Department<br>School<br>Employment<br>Years of Employment<br>Do you have a smartphone?<br>How many years have you used it?<br>How many years have you used computers?<br>How many years have you used the Internet? |
|                  | <b>Adapted from Androulidakis and Kandus (2011b)</b><br>BEH1. I am currently using a password on my smartphone.<br>BEH2. I change my password regularly on my smartphone.  |

|                               |  |
|-------------------------------|--|
| <p>Security<br/>Behavior</p>  | <p>BEH3. I always use a strong password that is hard to guess on my smartphone.</p> <p>BEH4. I am currently using anti-virus/anti-spyware on my smartphone.</p> <p>BEH5. I update the anti-virus/anti-spyware regularly on my smartphone.</p> <p>BEH6. I make a backup of my files regularly on my smartphone.</p> <p>BEH7. I download software only from well-known and secure sources to my smartphone.</p> <p>BEH8. I currently keep sensitive personal data on my smartphone.</p>  |
| <p>Security<br/>Intention</p> | <p><b>Adapted from Ng and Rahim (2005)</b></p> <p>INT1. I intend to put a password on my smartphone within the next month.</p> <p>INT2. I strongly intend to change my password on my smartphone regularly every month.</p> <p>INT3. I intend to use anti-virus/anti-spyware on my smartphone within the next month.</p> <p>INT4. It is my strong intention to update the anti-virus/anti-spyware on my smartphone regularly every month.</p> <p>INT5. I intend to make a backup of my important files on my smartphone within the next month.</p> <p>INT6. I strongly intend to make a backup of my important files on my smartphone within the next month.</p> |
| <p>Security<br/>Attitude</p>  | <p><b>Adapted from Taylor and Todd (1995a)</b></p> <p>ATT1. Putting a password on my smartphone is a good idea.</p> <p>ATT2. Updating my password on my smartphone is a good idea.</p> <p>ATT3. Using anti-virus/anti-spyware on my smartphone would be wise.</p> <p>ATT4. Updating anti-virus/anti-spyware regularly would be wise.</p> <p>ATT5. Backing up my important data regularly on my smartphone is a good idea.</p>  |

|                              |  |
|------------------------------|--|
|                              | ATT6. Backing up my important data regularly on my smartphone would be wise.   |
| Subjective Norm              | <p><b>Adapted from Taylor and Todd (1995c) and Ng and Rahim (2005)</b></p> <p>SN1. I would follow the advice of people (peers, family, professors, managers ...) that are important to me if they recommend I use a password on my smartphone and update it regularly.</p> <p>SN2. I would follow the advice of sources (School, Job, Internet ...) that are important to me if they recommend that I need to use password on my smartphone and update it regularly.</p> <p>SN3. I would follow the advice of people (peers, family, professors, managers ...) that are important to me if they recommend that I should use anti-virus/anti-spyware on my smartphone and update it regularly.</p> <p>SN4. I would follow the advice of sources (School, Job, Internet ...) that are important to me if they recommend that I need to use anti-virus/anti-spyware on my smartphone and update it regularly.</p> <p>SN5. If people (peers, family, professors, managers ...) that are important to me recommend it, I would make a backup of my important data regularly on my smartphone.</p> <p>SN6. If sources (Internet, mass media ...) that are important to me recommend that I need to make a backup of my important data on my smartphone regularly, I would do it.</p> |
| Perceived Behavioral Control | <p><b>Adapted from Taylor and Todd (1995c)</b></p> <p>PBC1. It is entirely within my control to set a password on my smartphone and update it regularly.</p> <p>PBC2. I have the resources, the knowledge, and the ability to put a password on my smartphone and update it regularly.</p> <p>PBC3. It is entirely within my control to use an anti-virus/anti-spyware on my smartphone and update it regularly.</p> <p>PBC4. I have the resources, the knowledge, and the ability to use anti-virus/anti-spyware on my smartphone and update it regularly.</p>  |

|                       |  |
|-----------------------|--|
|                       | <p>PBC5. It is entirely within my control to make a backup of my important data on my smartphone regularly.</p> <p>PBC6. I have the resources, the knowledge, and the ability to make a backup of my important data on my smartphone regularly.</p>  |
| Perceived Usefulness  | <p><b>Adapted from Taylor and Todd (1995c) and Ng and Rahim (2005)</b></p> <p>PU1. Setting a password and updating it regularly is useful and effective in securing my smartphone and preventing unauthorized access.</p> <p>PU2. Setting a password and updating it regularly on my smartphone is advantageous.</p> <p>PU3. Using anti-virus/anti-spyware and updating it regularly is useful and effective in securing my smartphone and preventing virus/spyware attacks.</p> <p>PU4. Making a backup of my important files on my smartphone regularly is useful and beneficial in protecting me against data loss.</p> <p>PU5. Making a backup of my important files on my smartphone regularly is advantageous.</p> |
| Perceived Ease of Use | <p><b>Adapted from Taylor and Todd (1995c)</b></p> <p>PEU1. It is easy to set a password on my smartphone</p> <p>PEU2. It is easy to update my password regularly on my smartphone.</p> <p>PEU3. It is easy to use anti-virus/anti-spyware on my smartphone.</p> <p>PEU4. It is easy to update anti-virus/anti-spyware regularly on my smartphone.</p> <p>PEU5. It is easy to make a backup of my important data on my smartphone.</p>   |
| Perceived             | <p><b>Adapted from Johnston and Warkentin (2010)</b></p> <p>PP1. It is possible that my smartphone will be accessed by unauthorized people.</p> <p>PP2. My smartphone is at risk for unauthorized access.</p>  |

|                    |   |
|--------------------|---|
| Probability        | <p>PP3. It is likely that my smartphone will become infected with virus/spyware.</p> <p>PP4. My smartphone is at risk of getting infected with virus/spyware.</p> <p>PP5. It is possible that I could lose my smartphone with my important data on it.</p> <p>PP6. My smartphone and the important data on it are at risk of getting lost.</p>  |
| Perceived Severity | <p><b>Adapted from Johnston and Warkentin (2010)</b></p> <p>PS1. If my smartphone were accessed by unauthorized people, it would be sever and serious problem for me.</p> <p>PS2. If my smartphone were accessed by unauthorized people, it would be risky for me.</p> <p>PS3. If my smartphone were infected by virus/spyware, it would be sever and serious problem for me.</p> <p>PS4. If my smartphone were infected by virus/spyware, it would be risky for me.</p> <p>PS5. If I lose my smartphone or lose my important data on it, it would be a severe and serious problem for me.</p> <p>PS6. If I lose my smartphone or lose my important data on it, it would be risky for me.</p> |
| People's Influence | <p><b>Adapted from Taylor and Todd (1995c)</b></p> <p>PI1. My peers suggest that I set a password on my smartphone and update it regularly.</p> <p>PI2. My family encourages me to set a password on my smartphone and update it regularly.</p> <p>PI3. My professors/supervisors recommend that I set a password on my smartphone and update it regularly.</p> <p>PI4. My peers suggest that I use anti-virus/anti-spyware on my smartphone and update it regularly.</p> <p>PI5. My family encourages me to use anti-virus/anti-spyware on my</p>  |



|                              |  |
|------------------------------|--|
|                              | <p>smartphone and update it regularly.</p> <p>PI6. My professors/supervisors recommend that I use anti-virus/anti-spyware on my smartphone and update it regularly.</p> <p>PI7. My peers suggest that I backup of my important data on my smartphone.</p> <p>PI8. My family encourages me to get a backup of my important files on my smartphone regularly.</p> <p>PI9. My professors/supervisors recommend that I backup of my important files on my smartphone regularly.</p>  |
| <p>Media's<br/>Influence</p> | <p><b>Adapted from Taylor and Todd (1995c) and Ng and Rahim (2005)</b></p> <p>MI1. Mass media (e.g., the Internet) suggests that I have to set a password on my smartphone and update it regularly.</p> <p>MI2. Mass media (e.g., TV and Newspaper) encourages me to set a password and update my password regularly.</p> <p>MI3. Mass media (e.g., the Internet) encourages me to use anti-virus/anti-spyware on my smartphone and update it regularly.</p> <p>MI4. Mass media (e.g., TV and Newspaper) suggests that I have to use anti-virus/anti-spyware and update it regularly.</p> <p>MI5. Mass media (e.g., the Internet) suggests that I backup my important data on my smartphone.</p> <p>MI6. Mass media (e.g., TV and Newspaper) encourages me to back up my important files on my smartphone regularly.</p> |
| <p>Self-Efficacy</p>         | <p><b>Adapted from Taylor and Todd (1995c)</b></p> <p>SE1. I feel confident that I can set a password and change it regularly on my smartphone on my own.</p> <p>SE2. I feel confident in learning how to set a password and change it regularly on my smartphone.</p> <p>SE3. I feel confident that I can use anti-virus/anti-spyware and can update it regularly on my smartphone.</p> <p>SE4. I feel confident in learning how to use anti-virus/anti-spyware</p>   |

|                           |   |
|---------------------------|---|
|                           | <p>and can update it regularly on my smartphone.</p> <p>SE5. I feel confident that I can back up my important files on my smartphone.</p> <p>SE6. I feel confident learning how to back up my important files on my smartphone.</p>   |
| Facilitation<br>Condition | <p><b>Adapted from Taylor and Todd (1995c)</b></p> <p>FC1. I have the time and resources to set a password on my smartphone and update it regularly.</p> <p>FC2. I have the time and resources to use anti-virus/antispyware on my smartphone and update it regularly.</p> <p>FC3. I have the time and resources to back up my important files on my smartphone.</p>  |
| Computing<br>Experience   | <p><b>Adapted from Rhee, Kim and Ryu (2009) and Benenson, Kroll-Peters and Krupp (2012)</b></p> <p>CE1. How would you evaluate your computing literacy level?</p> <p>CE2. How would you evaluate your Internet literacy level?</p> <p>CE3. How would you evaluate your smartphone literacy level?</p> <p>CE4. How would you rate your knowledge about information security?</p> <p>CE5. How would you rate your knowledge about protecting your smartphone?</p> |
| Breach<br>Experience      | <p><b>Adapted from Rhee, Kim and Ryu (2009)</b></p> <p>BE1. Has your smartphone ever been accessed by unauthorized people?</p> <p>BE2. Have you lost your smartphone or important files on your smartphone in past two years?</p> <p>BE3. Have you had a virus/spyware on your smartphone during the last two years?</p>  |

## **Instrument Validity**

Due to the fact that each construct is measured by multiple items, assessment of construct validity is essential. Construct validity will ensure that items within each construct are addressing the main construct. In this research, construct validity is determined by content validity, convergent validity, and discriminant validity.

Content validity is the degree to which the content of a questionnaire covers the extent and depth of the construct it is intended to cover (Akarapanich, 2006, p. 74). According to Ng, Kankanhalli and Xu (2009), content validity is ensured by adapting a questionnaire that is been used and validated in previous studies. This study ensures the content validity of its survey's questionnaire by extensively reviewing the literature and selecting scales that have been used and tested in similar environments. This study also ensured content validity by consulting with the following experts: three information security professors at Eastern Michigan University; three experts in the field of information security; and four committee members.

Convergent validity is established when variables that are theoretically expected to be similar within each construct are inter correlated. In contrast, discriminant validity is determined when variables that are theoretically expected to be different, are not correlated (DeVellis, 2011). While the items in one construct should be highly correlated, those items should have lower correlations with items that belong to other constructs. In order to test the convergent validity, items within a construct should have high significant factor loadings (*t-value*>1.96) while the construct should have high average variance extracted, AVE>0.5, and high level of reliability, Composite reliability>0.7 (Bagozzi & Heatherton, 1994; Esmaili & Eydgahi, 2013; Grace, Weaven, Bodey, Ross, & Weaven, 2012).

Finally, in order to test the discriminant validity, this study will adapt methodology described by Fornell and Larckers (1981). According to the authors, discriminant validity will be satisfied if the average variance extracted (AVE) is greater than the square of the construct's correlations with the other factors.

### **Pilot Test**

After ensuring the content validity of the developed survey, the reliability of the survey was tested through a pilot test to make sure that the survey was readable and reliable. One of the main goals of the pilot test was to ensure the survey was usable and that subjects did not have any problems responding to the survey. The pilot test involved distributing copies of the survey to be completed by students in an undergraduate class at Eastern Michigan University. The students also were encouraged to provide feedback to the investigator regarding modifications (changes, additions, deletions) to the design and readability of the survey.

### **Scale Reliability**

According to Straub (1989), reliability refers to evaluation of an instrument's reproducibility. The reliability of construct items will be ensured if respondents' results are internally consistent (e.g., Cronbach's alpha coefficient) and/or consistent over time such as test-retest reliability (Clarke, 2011). The author states the instrument is reliable if another researcher can achieve the same results by using the same methodology with subjects from the same population.

Many authors (e.g., Sprinthall & Fisk, 1990; Clarke, 2011) report that Cronbach's alpha coefficient ensures a scale's internal consistency reliability if the value of alpha for each major factor exceeds 0.7 (Park & Chen, 2007). The present study utilized the

Statistical Package for Social Science software (SPSS) to calculate Cronbach's alpha values for each of the survey's constructs. Test-retest reliability for consistency over time could not be evaluated in the current study since each respondent completed the survey only once.

### **Human Subjects**

This study selected its sample from among students at Eastern Michigan University and then utilized snowball sampling to increase the sample size. Since this study focused on human behavior, it required review and approval by the Human Subjects' Committee at Eastern Michigan University. Human subject approval ensured that the subjects would not experience any harm from their participation in this study, that the study would not collect any information that could identify them individually, and that the results would be reported only in a group format and used strictly for research purposes. Since participants had to access the survey questionnaire voluntarily online, their completion of the survey was considered evidence of their willingness to participate.

### **Data Collection**

This research utilized an online survey tool (LimeSurvey) that is hosted on EMU's servers to design a questionnaire. The designed survey was available through the Web and subjects could access the survey online. Moreover, the study did not collect any personal information from users to protect respondents' privacy.

A cover letter that explained the general purpose of this research along with an electronic link to the survey was sent to the students in several undergraduate classes through e-mail. Moreover, the subjects were encouraged to distribute information on how to access

the online survey to others. Data was collected over a period of two semesters to increase the return rate and sample size.

### **Data Analysis**

The data analysis was performed in three phases. In phase one, the collected data from the online survey tool, transferred to intermediate software such as Microsoft Excel for data-cleaning purposes. At this stage, the following tasks had be performed:

- (1) Incomplete surveys were discarded.
- (2) The researcher visually checked for any errors in the collected data such as more than one response to a single item.
- (3) The demographic and experience items were coded; e.g., for gender, 1 = male and 2 = female.

In the second phase, this study examined the reliability and validity of the main factors in the following manner:

- (1) The data were transferred into the SPSS data base.
- (2) Descriptive analyses such as mean, median, variance, standard deviation, kurtosis, and skew calculated to examine data quality.
- (3) The Cronbach's Alpha Coefficient Value was calculated for each construct. If any of the constructs showed a Cronbach's alpha value  $> 0.7$ , further investigation was conducted to ensure the internal consistency of the constructs.
- (4) Confirmatory Factor Analysis (CFA) was calculated to ensure the constructs' validity and to regroup the items in the new constructs if needed.

Finally in the last step, the data were transferred to Smart PLS software. Smart PLS can generate and recognize two main models: a measurement model and a structural model

(Jones, McCarthy, Halawi, & Mujtaba, 2010). The bootstrapping function within SmartPLS measures items loading within each factor in the form of t-values that are used to examine the significance of each question. Items showing t-values lower than 1.96 in reflective models were eliminated from the analysis (Chin, 1998). For these reasons, the measurement model along with bootstrapping was used to examine the construct validity. The structural model was used to test the hypotheses. In the structural model, Smart PLS calculated the path coefficient and the size of the R-squared value for each hypothesis.

### **Summary**

This chapter provided a detailed description of all steps in the research methodology that was used in this study, including the research design, population, and sampling, instrument development, human subject approval, pilot test description, reliability, validity tests, and data collection and data analysis plans. The next chapter will provide the results of the implementation of this research methodology.

## **Chapter 4. Results**

This chapter provides the detailed results of the statistical analysis of the collected data through the research survey. This chapter starts with analyzing the return rate of the survey and demographic. After analyzing the demographic, this study examined the reliability and validity of the developed survey. Finally, this study utilized statistical tools such as SPSS and SmartPLS to examine the research hypotheses.

The data collection started in Fall 2013 and continued through the Winter 2014 term, for a duration of two semesters. Due to school policy, this study could not send a mass email to all subjects. For this reason, with help from the IT department at Eastern Michigan University the link to the survey along with a consent letter was posted at school's Website daily announcements and the Eastern Michigan University's Facebook page. Also, the researcher contacted several faculties within the School of Technology and asked them to share the survey with their students. In most of the classes, taking the survey was optional and in some classes, professors provided extra credit to motivate the students to take the survey.

### **Completion Rates**

This study utilized convenient sampling along with snowball sampling to increase the return rate. From a total of 841 responses, 593 responses were completed and 248 responses were incomplete. In other words, 70.5 % of the total respondents completed the survey and only 29.5 % of responses were not completed.



## Demographic Characteristics of the Sample

This study collected the following demographic characteristics: age, gender, education level, number of education years after high school, major, school, employment, years of employment, smartphone ownership, and years of smartphone use. Based upon the type of demographic variables the demographic characteristics of the sample are presented in three categories: nominal, categorical, and scale.

Table 2 illustrates the nominal variable of gender, employment status, and smartphone ownership. From the 593 respondents, 325 were male, representing 54.8 percent of the sample and 268 were female, representing 45.2 percent of the sample. Also, 70 percent of the participants were employed and 30 percent of the respondents reported that they were not employed. Finally, Table 2 shows that 94.8 percent of the participants owned a smartphone, which is very significant and highlights the importance of this study.

Table 2

### *Demographic characteristics of the sample*

|                             |                        |                          |
|-----------------------------|------------------------|--------------------------|
| <b>Gender</b>               | <b>Male</b><br>54.8%   | <b>Female</b><br>45.2%   |
| <b>Employment Status</b>    | <b>Employed</b><br>70% | <b>Unemployed</b><br>30% |
| <b>Smartphone Ownership</b> | <b>Yes</b><br>94.8%    | <b>No</b><br>5.2%        |

Table 3 illustrates the education level of the participants. According to the collected data, 14.3 % of the participants held an Associate's degree, 22.6% Bachelor degree, 9.3% had high school diploma, 24.3% had a master's degree, 2.2% had earned a PhD and 27.3% had some college or tech school.

Table 3

*Education Level*

|                          | <b>Frequency</b> | <b>Percent</b> | <b>Cumulative<br/>Percent</b> |
|--------------------------|------------------|----------------|-------------------------------|
| High School Diploma/GED  | 55               | 9.3            | 9.3                           |
| Some College/Tech School | 162              | 27.3           | 36.6                          |
| Associate Degree         | 85               | 14.3           | 50.9                          |
| Bachelor Degree          | 134              | 22.6           | 73.5                          |
| Master                   | 144              | 24.3           | 97.8                          |
| PhD                      | 13               | 2.2            | 100.0                         |
| Total                    | 593              | 100.0          |                               |

Finally Table 4 represents the rest of the demographics such as age, years of education after high school, number of employment years, and the number of the years that participants have used a smartphone. The average age of the participants was 28; the average number of years of education after high school was 5 years; the average years of employment was 7.89 and the average of the number of years that samples had used a smartphone was 3.4 years.

Table 4

*Demographic Characteristics*

|                                      | <b>N</b> | <b>Mini</b> | <b>Max</b> | <b>Mean</b> | <b>Std. Deviation</b> | <b>Variance</b> |
|--------------------------------------|----------|-------------|------------|-------------|-----------------------|-----------------|
| Age                                  | 593      | 16          | 70         | 28.77       | 10.755                | 115.675         |
| Years of education after high school | 593      | .0          | 22.0       | 4.964       | 3.5118                | 12.333          |
| Years of Employment                  | 593      | .0          | 51.0       | 7.897       | 9.3021                | 86.528          |
| Year of smartphone use               | 593      | .0          | 15.0       | 3.461       | 2.3290                | 5.424           |
| Valid N (listwise)                   | 593      |             |            |             |                       |                 |

To measure if the users of smartphone saved sensitive data on their devices, this study asked each person to answer the following question using a Likert-type scale: I currently keep sensitive personal data in my smartphone (BEH8). From 593 responses, 35.9% of the sample size declared that they saved sensitive data on their devices, while only 45.5 % of users had password (BEH1) on their devices; 14.9% (BEH4) used antivirus software; and just 19.1% of the users were strongly agreed that they regularly back up of their files (BEH6).

### **Assessment of Measures**

The data analysis involved six steps including pilot test analysis, reliability analysis, descriptive analysis, normality, factor analysis, and hypothesis testing.

**Pilot and feedback analysis.** The pilot test was used to collect the participants' feedback regarding the readability and clarity of the investigator-developed survey. After collecting the pilot study, this study performed a reliability analysis to ensure that the survey was reliable. Also, this study required participants to validate their answers by answering questions such as: “the questions were clear and readable”; “the survey was well designed”; and “my responses were honest and complete.” This research used a Likert scale between 1 and 5, where 1 represented “strongly disagree” and 5, “strongly agree” to collect the feedback questions. The distribution of responses is summarized in Table 5.

Table 5

*Respondents' feedback*

|                           | <b>Strongly Disagree</b> | <b>Disagree</b> | <b>Neutral</b> | <b>Agree</b> | <b>Strongly Agree</b> |
|---------------------------|--------------------------|-----------------|----------------|--------------|-----------------------|
| Survey clear and readable | 2.5%                     | 6.9%            | 14.5%          | 37.1%        | 39.0%                 |
| Survey is well designed   | 5.9%                     | 13.5%           | 23.9%          | 28.8%        | 27.8%                 |
| My responses were honest  | 0.3%                     | 1.2%            | 4.4%           | 19.4%        | 74.7%                 |

The responses revealed that the subjects responded honestly to the survey and a majority of the respondents believed that the survey questions were clear and well designed.

**Descriptive and reliability analysis.** In order to examine the reliability of the developed survey this study examined Cronbach's alpha coefficient, which represents the internal consistency reliability of items. According to Park and Chen (2007), a value of 0.7 or above is desirable. Cronbach's alpha ( $\alpha$ ) was calculated utilizing SPSS. The results are summarized in Table 6. All of the variables show high levels of internal consistency reliability, i.e.,  $\alpha > 0.7$ .

Each construct consisted of several items and each item was assessed using a five-point Likert-type scale: Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4), and Strongly Agree (5). Since each construct was generated from a summation of several Likert-type items, this study treated each construct as an interval variable and provided descriptive statistics for each construct, i.e., mean, variance, standard deviation (Boone and Boone, 2012). Also, to analyze each item within a construct, item means, item variances, inter-item correlations, item-total statistics, etc. were calculated. The analysis of each scale including Mean and Standard Deviation presented in Table 6. Also, the analysis of items within each

constructs demonstrated that deletion of none of the items within each construct would significantly improve the overall reliability for each construct.

Table 6

*Cronbach's Alpha for constructs (N=593)*

| Variable                     | Descriptive Analysis |                    | Reliability Statistics |                  |
|------------------------------|----------------------|--------------------|------------------------|------------------|
|                              | Mean                 | Standard Deviation | Number of Items        | Cronbach's Alpha |
| Security Behavior            | 23.02                | 7.07               | 8                      | 0.779            |
| Security Intention           | 17.7                 | 6.098              | 6                      | 0.853            |
| Security Attitude            | 23.80                | 4.724              | 6                      | 0.867            |
| Subjective Norm              | 21.04                | 5.524              | 6                      | 0.909            |
| Perceived Behavioral Control | 24.94                | 4.889              | 6                      | 0.874            |
| Perceived Usefulness         | 20.07                | 3.993              | 5                      | 0.875            |
| Perceived Ease of Use        | 19.19                | 4.329              | 5                      | 0.832            |
| Perceived Probability        | 17.34                | 5.919              | 6                      | 0.896            |
| Perceived Severity           | 19.18                | 6.418              | 6                      | 0.993            |
| People's Influence           | 29.80                | 8.637              | 9                      | 0.939            |
| Media's Influence            | 20.30                | 6.046              | 6                      | 0.938            |
| Self-Efficacy                | 23.48                | 5.377              | 6                      | 0.890            |
| Facilitation Condition       | 11.70                | 2.915              | 3                      | 0.816            |
| Breach Experience            | 9.90                 | 4.812              | 5                      | 0.858            |
| Computing Experience         | 19.68                | 3.835              | 5                      | 0.864            |

This study provided more detailed descriptive analysis in Appendix C. In Appendix C, after describing and providing details about each construct, this section reports the following sections for each scale and its items analysis from SPSS output:

- Statistics for Scale: Including Mean, Variance, and Standard Deviation of the construct.

- Item Statistics: Including Mean, Variance, and Standard Deviation for each item related to the construct.
- Summary Item Statistics: Including Means, Variances, and Inter-Item Correlations for the set of items within a construct.
- Item-total Statistics: Including “Scale Mean if Item Deleted,” “Scale Variance if Item Deleted,” “Corrected Item-Total Correlation,” “Squared Multiple Correlation,” and “Cronbach's Alpha if Item Deleted.”

**Normality.** This study has utilized Skewness and Kurtosis to examine the data normality. Normally distributed data have a Skewness and Kurtosis range between +2 to -2 (Kline, 2011). If the Skewness falls out of the normal range, the data is not symmetric; if the Kurtosis falls out of the normal range, the distribution of the data is either narrowed or widened. There are several techniques to modify the data that is not normally distributed into normally distributed data. As presented in Table 7, the value of Kurtosis in four items of PCB1, PCB2, PCB5, and PEU 1 is positive and above the acceptable range. For this reason this study utilized the transformation formula of  $\text{Sin}(\text{Sqrt}(x))$  to normalize the collected data (Kline, 2011). Also, the values of Skewness and Kurtosis after transformation have been presented in Table 7.

Table 7

*Normality Analysis*

| No | Items | Before Transformation |          | After Transformation |          |
|----|-------|-----------------------|----------|----------------------|----------|
|    |       | Skewness              | Kurtosis | Skewness             | Kurtosis |
| 1  | BEH1  | -.417                 | -1.566   | .790                 | -.899    |
| 2  | BEH2  | .875                  | -.283    | .830                 | -.808    |
| 3  | BEH3  | .015                  | -1.436   | -.126                | -1.679   |
| 4  | BEH4  | .597                  | -.998    | .001                 | -1.489   |
| 5  | BEH5  | .679                  | -.812    | .065                 | -1.629   |
| 6  | BEH6  | -.085                 | -1.320   | .024                 | -1.655   |
| 7  | BEH7  | -.903                 | .012     | -.210                | -1.422   |
| 8  | BEH8  | .090                  | -1.233   | -.044                | -1.440   |
| 9  | IN1   | -.003                 | -1.124   | -.336                | -1.321   |
| 10 | IN2   | .417                  | -.905    | -.390                | -1.429   |
| 11 | IN3   | .217                  | -1.177   | -.503                | -1.364   |
| 12 | IN4   | .268                  | -1.115   | -.321                | -1.457   |
| 13 | IN5   | -.407                 | -.955    | -.350                | -1.476   |
| 14 | IN6   | -.326                 | -1.105   | -.294                | -1.351   |
| 15 | ATT1  | -1.240                | 1.147    | -.214                | -1.445   |
| 16 | ATT2  | -.690                 | -.072    | .312                 | -1.467   |
| 17 | ATT3  | -.629                 | -.264    | -.226                | -1.475   |
| 18 | ATT4  | -.681                 | -.118    | -.264                | -1.476   |
| 19 | ATT5  | -1.274                | 1.931    | -.262                | -1.434   |
| 20 | ATT6  | -1.214                | 1.634    | .107                 | -1.420   |
| 21 | SN1   | -.328                 | -.703    | .065                 | -1.424   |
| 22 | SN2   | -.676                 | -.238    | -.660                | -.933    |
| 23 | SN3   | -.182                 | -.697    | -.345                | -1.273   |
| 24 | SN4   | -.320                 | -.572    | -.779                | -.817    |
| 25 | SN5   | -.584                 | -.189    | -.656                | -1.009   |
| 26 | SN6   | -.601                 | -.248    | -.530                | -1.015   |
| 27 | PBC1  | -1.920                | 3.959    | -.455                | -1.154   |
| 28 | PBC2  | -1.778                | 3.131    | .754                 | -.974    |
| 29 | PBC3  | -.975                 | .060     | .168                 | -1.553   |
| 30 | PBC4  | -.647                 | -.772    | .020                 | -1.588   |
| 31 | PBC5  | -1.558                | 2.574    | .489                 | -1.280   |
| 32 | PBC6  | -1.230                | .816     | .338                 | -1.451   |
| 33 | PU1   | -1.171                | 1.223    | .118                 | -1.466   |

|    |      |        |        |       |        |
|----|------|--------|--------|-------|--------|
| 34 | PU2  | -.873  | .251   | -.109 | -1.465 |
| 35 | PU3  | -.658  | -.005  | -.332 | -1.366 |
| 36 | PU4  | -1.142 | 1.375  | .114  | -1.457 |
| 37 | PU5  | -1.057 | 1.003  | .077  | -1.485 |
| 38 | PEU1 | -1.753 | 3.065  | .666  | -1.080 |
| 39 | PEU2 | -1.492 | 1.986  | .498  | -1.297 |
| 40 | PEU3 | -.225  | -.911  | -.477 | -1.386 |
| 41 | PEU4 | -.274  | -.902  | -.418 | -1.445 |
| 42 | PEU5 | -.789  | -.243  | -.042 | -1.573 |
| 43 | PP1  | -.240  | -1.088 | -.556 | -.872  |
| 44 | PP2  | .118   | -1.061 | -.691 | -.915  |
| 45 | PP3  | .420   | -.563  | -.819 | -.923  |
| 46 | PP4  | .291   | -.846  | -.698 | -1.022 |
| 47 | PP5  | -.391  | -.923  | -.462 | -1.032 |
| 48 | PP6  | -.090  | -1.079 | -.568 | -1.024 |
| 49 | PS1  | .130   | -1.100 | -.710 | -.994  |
| 50 | PS2  | -.077  | -1.130 | -.631 | -.965  |
| 51 | PS3  | -.353  | -.808  | -.582 | -.986  |
| 52 | PS4  | -.384  | -.771  | -.569 | -.969  |
| 53 | PS5  | -.171  | -1.075 | -.584 | -1.065 |
| 54 | PS6  | -.153  | -1.107 | -.585 | -1.048 |
| 55 | PI1  | -.418  | -.658  | -.556 | -1.048 |
| 56 | PI2  | -.244  | -.908  | -.569 | -1.114 |
| 57 | PI3  | -.354  | -.754  | -.528 | -1.178 |
| 58 | PI4  | -.094  | -.753  | -.833 | -.697  |
| 59 | PI5  | -.070  | -.858  | -.753 | -.844  |
| 60 | PI6  | -.197  | -.678  | -.747 | -.869  |
| 61 | PI7  | -.511  | -.414  | -.605 | -.864  |
| 62 | PI8  | -.384  | -.650  | -.572 | -1.066 |
| 63 | PI9  | -.530  | -.433  | -.497 | -1.108 |
| 64 | MI1  | -.495  | -.604  | -.466 | -1.171 |
| 65 | MI2  | -.272  | -.799  | -.647 | -1.008 |
| 66 | MI3  | -.272  | -.733  | -.679 | -.924  |
| 67 | MI4  | -.116  | -.800  | -.824 | -.691  |
| 68 | MI5  | -.517  | -.461  | -.517 | -1.083 |
| 69 | MI6  | -.335  | -.692  | -.646 | -.954  |
| 70 | SE1  | -1.285 | 1.198  | .274  | -1.437 |
| 71 | SE2  | -1.337 | 1.475  | .316  | -1.418 |



|    |     |        |       |       |        |
|----|-----|--------|-------|-------|--------|
| 72 | SE3 | -.499  | -.798 | -.263 | -1.439 |
| 73 | SE4 | -.578  | -.708 | -.188 | -1.498 |
| 74 | SE5 | -.999  | .264  | .109  | -1.538 |
| 75 | SE6 | -1.061 | .494  | .126  | -1.514 |
| 76 | FC1 | -1.441 | 1.679 | .416  | -1.346 |
| 77 | FC2 | -.572  | -.688 | -.152 | -1.563 |
| 78 | FC3 | -.880  | -.020 | -.024 | -1.519 |
| 79 | BE1 | 1.134  | .375  | .059  | -1.734 |
| 80 | BE2 | .804   | -.667 | .159  | -1.550 |
| 81 | BE3 | 1.160  | .344  | .205  | -1.677 |
| 82 | BE4 | 1.209  | .242  | .401  | -1.472 |
| 83 | BE5 | 1.380  | 1.168 | .311  | -1.691 |
| 84 | CE1 | -.865  | .547  | .138  | -1.473 |
| 85 | CE2 | -1.028 | 1.169 | .281  | -1.416 |
| 86 | CE3 | -.869  | .477  | -.138 | -1.429 |
| 87 | CE4 | -.335  | -.662 | -.595 | -1.112 |
| 88 | CE5 | -.377  | -.638 | -.522 | -1.242 |

**Factor analysis.** Factor analysis is methodology that could be used to group items together and form new constructs. Also, this analysis could be used to examine the coherence of the items in each construct. In other words, factor analysis will ensure that underlying items are highly correlated with each other and have been influenced by the measured construct. According to DeCoster (1988), “Measures that are highly correlated are likely influenced by the same factors, while those that are relatively uncorrelated are likely influenced by different factors” (p. 1).

The factor analysis could be classified into two main types: Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA). In exploratory factor analysis, the analysis would start with ungrouped items to identify groups of items and form new constructs. By comparison, confirmatory factor analysis starts with a few constructs and

examines the linkages of the items with the underlying constructs that have been defined by researchers (Anderson & Gerbing, 1998).

Since this study has selected its constructs and formed items from the literature, it uses confirmatory factor analysis to examine the coherence of the items within each construct. Also, the PLS-SEM has been used to examine the measurement model validity and reliability, in cases where latent variable scores are used in subsequent analyses (Hair, Sarstedt, Ringle, & Mena, 2012).

According to Costello and Osboren (2005), although factor loadings greater than 0.5 are significant and acceptable, in confirmatory factor analysis, factor loadings greater than 0.7 are considered very significant. As illustrated in Table 8 only BEH6, BEH7, and BEH8 have factor loadings lower than 0.5 which shows that this factor is not related to the main construct. For this reason, this factor has been eliminated from future analysis.

Table 8

*Factor Loading*

| <b>Item</b> | <b>Question</b>   | <b>Construct</b>  | <b>Factor Loading</b> |
|-------------|---|-------------------|-----------------------|
| BEH1        | I am currently using a password on my smartphone.                             | Security Behavior | 0.6586                |
| BEH2        | I change my password regularly on my smartphone.                              |                   | 0.7429                |
| BEH3        | I always use a strong password that is hard to guess on my smartphone.        |                   | 0.7358                |
| BEH4        | I am currently using anti-virus/anti-spyware on my smartphone.                |                   | 0.6857                |
| BEH5        | I update the anti-virus/anti-spyware regularly on my smartphone.              |                   | 0.7168                |
| BEH6        | I make a backup of my files regularly on my smartphone.                       |                   | 0.4646                |
| BEH7        | I download software only from well-known and secure sources to my smartphone. |                   | 0.3472                |

|      |   |                    |        |
|------|---|--------------------|--------|
| BEH8 | I currently keep sensitive personal data in my smartphone.  |                    | 0.3345 |
| IN1  | I intend to put a password on my smartphone within the next month.  | Security Intention | 0.7096 |
| IN2  | I strongly intend to change my password on my smartphone regularly every month.   |                    | 0.7696 |
| IN3  | I intend to use anti-virus/anti-spyware on my smartphone within the next month.   |                    | 0.7888 |
| IN4  | It is my strong intention to update the anti-virus/anti-spyware on my smartphone regularly every month.   |                    | 0.8006 |
| IN5  | I intend to make a backup of my important files on my smartphone within the next month.   |                    | 0.7201 |
| IN6  | I strongly intend to make a backup of my important files on my smartphone within the next month.  |                    | 0.7635 |
| ATT1 | Putting a password on my smartphone is a good idea.   | Security Attitude  | 0.7409 |
| ATT2 | Updating my password on my smartphone is a good idea.   |                    | 0.7802 |
| ATT3 | Using anti-virus/anti-spyware on my smartphone would be wise.   |                    | 0.7875 |
| ATT4 | Updating anti-virus/anti-spyware regularly would be wise.   |                    | 0.8056 |
| ATT5 | Backing up my important data regularly in my smartphone is a good idea.   |                    | 0.7761 |
| ATT6 | Backing up my important data regularly in my smartphone would be wise.  |                    | 0.7652 |
| SN1  | I would follow the advice of people (peers, family, professors, managers ...) that are important to me if they recommend I use a password on my smartphone and update it regularly. | Subjective Norm    | 0.8029 |
| SN2  | I would follow the advice of sources (School, Job, Internet ...) that are important to me if they recommend that I need to use password on my smartphone and update it regularly.   |                    | 0.8356 |
| SN3  | I would follow the advice of people (peers, family, professors, managers ...) that are important to me if they  |                    | 0.8306 |

|      |  |                              |        |
|------|--|------------------------------|--------|
|      | recommend that I should use anti-virus/anti-spyware on my smartphone and update it regularly.  |                              |        |
| SN4  | I would follow the advice of sources (School, Job, Internet ...) that are important to me if they recommend that I need to use anti-virus/anti-spyware on my smartphone and update it regularly. |                              | 0.8539 |
| SN5  | If people (peers, family, professors, managers ...) that are important to me recommend it, I would make a backup of my important data regularly on my smartphone.                                |                              | 0.8202 |
| SN6  | If sources (Internet, mass media ...) that are important to me recommend that I need to make a backup of my important data on my smartphone regularly, I would do it.                            |                              | 0.8291 |
| PBC1 | It is entirely within my control to set a password on my smartphone and update it regularly.   | Perceived Behavioral Control | 0.7706 |
| PBC2 | I have the resources, the knowledge, and the ability to put a password on my smartphone and update it regularly.   |                              | 0.8202 |
| PBC3 | It is entirely within my control to use an anti-virus/anti-spyware on my smartphone and update it regularly.   |                              | 0.765  |
| PBC4 | I have the resources, the knowledge, and the ability to use anti-virus/anti-spyware on my smartphone and update it regularly.  |                              | 0.7339 |
| PBC5 | It is entirely within my control to make a backup of my important data on my smartphone regularly.   |                              | 0.8497 |
| PBC6 | I have the resources, the knowledge, and the ability to make a backup of my important data on my smartphone regularly.   |                              | 0.836  |
| PU1  | Setting a password and updating it regularly is useful and effective in securing my smartphone and preventing unauthorized access.   | Perceived Usefulness         | 0.8449 |
| PU2  | Setting a password and updating it regularly on my smartphone is advantageous.   |                              | 0.8329 |
| PU3  | Using anti-virus/anti-spyware and updating it regularly is useful and effective in securing my smartphone and preventing virus/spyware attacks.  |                              | 0.7407 |
| PU4  | Making a backup of my important files on my  |                              | 0.8424 |

|      |   |                       |        |
|------|---|-----------------------|--------|
|      | smartphone regularly is useful and beneficial in protecting me against data loss.                         |                       |        |
| PU5  | Making a backup of my important files on my smartphone regularly is advantageous.                         |                       | 0.8372 |
| PEU1 | It is easy to set a password on my smartphone   | Perceived Ease of Use | 0.8468 |
| PEU2 | It is easy to update my password regularly on my smartphone.  |                       | 0.8702 |
| PEU3 | It is easy to use anti-virus/anti-spyware on my smartphone.   |                       | 0.7013 |
| PEU4 | It is easy to update anti-virus/anti-spyware regularly on my smartphone.                                  |                       | 0.7023 |
| PEU5 | It is easy to make a backup of my important data on my smartphone.  |                       | 0.7184 |
| PP1  | It is possible that my smartphone will be accessed by unauthorized people.                                | Perceived Probability | 0.8014 |
| PP2  | My smartphone is at risk for unauthorized access.   |                       | 0.8368 |
| PP3  | It is likely that my smartphone will become infected with virus/spyware.                                  |                       | 0.807  |
| PP4  | My smartphone is at risk of getting infected with virus/spyware.  |                       | 0.8547 |
| PP5  | It is possible that I could lose my smartphone with my important data on it.                              |                       | 0.7683 |
| PP6  | My smartphone and important data on it are at risk of getting lost.                                       |                       | 0.7871 |
| PS1  | If my smartphone were accessed by unauthorized people, it would be a severe and serious problem for me.   | Perceived Severity    | 0.8589 |
| PS2  | If my smartphone were accessed by unauthorized people, it would be risky for me.                          |                       | 0.8621 |
| PS3  | If my smartphone were infected by virus/spyware, it would be a severe and serious problem for me.         |                       | 0.8557 |
| PS4  | If my smartphone were infected by virus/spyware, it would be risky for me.                                |                       | 0.8832 |
| PP5  | If I lose my smartphone or lose my important data on it, it would be a severe and serious problem for me. |                       | 0.7683 |
| PP6  | If I lose my smartphone or lose my important data on it, it   |                       | 0.872  |

|     |   |                    |        |
|-----|---|--------------------|--------|
|     | would be risky for me.  |                    |        |
| PI1 | My peers would suggest that I set a password on my smartphone and update it regularly.  | People's Influence | 0.822  |
| PI2 | My family would encourage me to set a password on my smartphone and update it regularly.  |                    | 0.8421 |
| PI3 | My professors/supervisors recommend that I set a password on my smartphone and update it regularly.                             |                    | 0.846  |
| PI4 | My peers would suggest that I should use anti-virus/anti-spyware on my smartphone and update it regularly.                      |                    | 0.8507 |
| PI5 | My family would encourage me to use anti-virus/anti-spyware on my smartphone and update it regularly.                           |                    | 0.8419 |
| PI6 | My professors/supervisors recommend that I use anti-virus/anti-spyware on my smartphone and update it regularly.                |                    | 0.8361 |
| PI7 | My peers would suggest that I backup my important data on my smartphone.  |                    | 0.7926 |
| PI8 | My family would encourage me to back up my important files on my smartphone regularly.  |                    | 0.7534 |
| PI9 | My professors/supervisors recommend that I backup my important files on my smartphone regularly.                                |                    | 0.785  |
| MI1 | The mass media (e.g., the Internet) suggests that I have to set a password on my smartphone and update it regularly.            | Media's Influence  | 0.8664 |
| MI2 | My mass media (e.g., TV, Newspaper) would encourage me to set a password and update my password regularly.                      |                    | 0.8919 |
| MI3 | The mass media (e.g., the Internet) would encourage me to use anti-virus/anti-spyware on my smartphone and update it regularly. |                    | 0.8636 |
| MI4 | The mass media (e.g., TV and Newspaper) would suggest that I have to use anti-virus/anti-spyware and update it regularly.       |                    | 0.8777 |
| MI5 | The mass media (e.g., the Internet) would suggest me to get a backup of my important data on my smartphone.                     |                    | 0.8687 |
| MI6 | The mass media (e.g., TV and Newspaper) would encourage me to get a backup of my important files on my smartphone regularly.    |                    | 0.8775 |

|     |  |                        |        |
|-----|--|------------------------|--------|
| SE1 | I feel confident that I can set a password and change it regularly in my smartphone on my own.         | Self-Efficacy          | 0.7891 |
| SE2 | I feel confident learning how to set a password and change it regularly on my smartphone.              |                        | 0.8216 |
| SE3 | I feel confident that I can use anti-virus/anti-spyware and update it regularly on my smartphone.      |                        | 0.7647 |
| SE4 | I feel confident learning how to use anti-virus/anti-spyware and update it regularly on my smartphone. |                        | 0.7929 |
| SE5 | I feel confident that I can back up my important files on my smartphone.                               |                        | 0.8362 |
| SE6 | I feel confident learning how to back up my important files on my smartphone.                          |                        | 0.8352 |
| FC1 | I have the time and resources to set a password on my smartphone and update it regularly.              | Facilitating Condition | 0.8383 |
| FC2 | I have the time and resources to use anti-virus/Antispyware on my smartphone and update it regularly.  |                        | 0.8491 |
| FC3 | I have the time and resources to back up my important files on my smartphone.                          |                        | 0.8843 |
| CE1 | How would you evaluate your computing literacy level?  | Computing Experience   | 0.7788 |
| CE2 | How would you evaluate your Internet literacy level?   |                        | 0.7497 |
| CE3 | How would you evaluate your smartphone literacy level?   |                        | 0.7793 |
| CE4 | How would you rate your knowledge about information security?  |                        | 0.8492 |
| CE5 | How would you rate your knowledge about protecting your smartphone?                                    |                        | 0.871  |
| BE1 | Has your smartphone ever been accessed by unauthorized people?   | Breach Experience      | 0.7788 |
| BE2 | Have you ever lost your smartphone or important files on your smartphone during the last two years?    |                        | 0.7497 |
| BE3 | Have you ever had a virus/spyware on your smartphone during the last two years?                        |                        | 0.7793 |

**Construct validity.** Due to the fact that each construct has been measured by multiple items, assessment of construct validity is essential. Construct validity will ensure that items within each construct are addressing the main construct. In this research, construct validity was determined by content validity, convergent validity, and discriminant validity. Content validity is the degree to which the content of a questionnaire covers the extent and depth of the topics it is intended to cover (Akarapanich, 2006, p. 74). According to Ng, Kankanhalli and Xu (2009), content validity is ensured by adapting questionnaires that have been used and validated in previous studies. This study examined the content validity of its survey's questionnaire through an extensive review of the literature and by selecting the scales that have been used and tested in a similar environment before. This study ensured content validity by consulting with a panel of experts which was made up of three information security professors at Eastern Michigan University; three outside experts in the field of information security; and four committee members.

Convergent validity is established when variables that are theoretically predicted to be correlated within a construct are, in fact, correlated. In contrast, discriminant validity is determined when variables that are theoretically predicted to differ, are not correlated (DeVellis, 2011). In other words, items within each construct should be highly correlated while the items in one construct should have less of a correlation with items that belong to other constructs. In order to test the convergent validity, constructs should have high significant factor loading ( $t\text{-value} > 1.96$ ); high Average Variance Extracted ( $AVE > 0.5$ ); and high level of reliability, Composite reliability  $> 0.7$ , (Esmaeili and Eydgahi, 2013; Dehghan, 2012; Grace, Weaven, Bodey, Ross, & Weaven, 2012; Bagozzi and Heatherton, 1994). According to Segars (1997), to justify using a construct, the average variance extracted



(AVE) which measures the variance captured by the indicators relative to measurement error, should be greater than 0.50. As presented in Table 9, the value of AVE in all of the constructs is larger than 0.5 and the calculated Composite Reliability is larger than 0.7. The results of the factor analysis along with values of AVE and Composite Reliability confirms that the constructs in the current survey have convergent validity.

Table 9

*Convergent Validity*

| <b>Constructs</b>                  | <b>AVE</b> | <b>Composite Reliability</b> | <b>Cronbachs Alpha</b> |
|------------------------------------|------------|------------------------------|------------------------|
| Security Attitude (ATT)            | 0.60       | 0.90                         | 0.87                   |
| Security Behavior (BEH)            | 0.50       | 0.84                         | 0.78                   |
| Facilitating Condition (FC)        | 0.74       | 0.89                         | 0.82                   |
| Security Intention (IN)            | 0.58       | 0.89                         | 0.85                   |
| Media's Influence (MI)             | 0.76       | 0.95                         | 0.94                   |
| Perceived Behavioral Control (PBC) | 0.64       | 0.91                         | 0.88                   |
| Perceived Ease of Use (PEU)        | 0.59       | 0.88                         | 0.84                   |
| People's Influence (PI)            | 0.67       | 0.95                         | 0.94                   |
| Perceived Probability (PP)         | 0.66       | 0.92                         | 0.89                   |
| Perceived Severity (PS)            | 0.75       | 0.95                         | 0.93                   |
| Perceive Usefulness (PU)           | 0.67       | 0.91                         | 0.88                   |
| Self-Efficacy (SE)                 | 0.65       | 0.91                         | 0.89                   |
| Subjective Norm (SN)               | 0.69       | 0.93                         | 0.91                   |
| Computing Experience (CE)          | 0.65       | 0.90                         | 0.87                   |
| Breach Experience (BE)             | 0.64       | 0.90                         | 0.86                   |

Finally, in order to test discriminant validity this study utilized the technique of PLS path modeling. Discriminant validity determines whether each latent variable shares more variances with its own manifest items than with other constructs (Fornell & Bookstein, 1982; Chin, 1998; Todorova, 2013). According to Fornell and Larckers (1981), discriminant validity can be established from the correlations among constructs and AVE. According to the authors, the discriminant validity will be satisfied if the square root of a construct's AVE is greater than the correlations between constructs (Koufteros, 1999; Koufteros, Vonderembse, & Doll, 2001). The results of the discriminant analysis of this study's survey results are presented in Table 10. The square roots of the AVE for each constructs have been placed in the diagonal of the table and the other cells represent the correlation between that construct and others. As demonstrated in Table 10, the value of the AVE for each constructs is larger than the correlations in its corresponding row and column, which satisfy the requirements for establishing discriminant validity.

Table 10

*Discriminant Validity Analysis*

|     | ATT          | BE           | BEH          | CE           | FC           | IN           | MI           | PBC          | PEU          | PI           | PP           | PS           | PU           | SE           | SN           |
|-----|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| ATT | <b>0.776</b> | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            |
| BE  | 0.040        | <b>0.799</b> | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            |
| BEH | 0.496        | 0.262        | <b>0.636</b> | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            |
| CE  | 0.244        | -0.054       | 0.302        | <b>0.807</b> | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            |
| FC  | 0.373        | 0.009        | 0.344        | 0.411        | <b>0.857</b> | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            |
| IN  | 0.531        | 0.223        | 0.616        | 0.233        | 0.300        | <b>0.759</b> | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            |
| MI  | 0.302        | 0.147        | 0.261        | 0.203        | 0.320        | 0.219        | <b>0.874</b> | 0            | 0            | 0            | 0            | 0            | 0            | 0            | 0            |
| PBC | 0.426        | -0.132       | 0.288        | 0.386        | 0.654        | 0.275        | 0.311        | <b>0.797</b> | 0            | 0            | 0            | 0            | 0            | 0            | 0            |
| PEU | 0.359        | -0.016       | 0.376        | 0.384        | 0.667        | 0.328        | 0.304        | 0.666        | <b>0.771</b> | 0            | 0            | 0            | 0            | 0            | 0            |
| PI  | 0.439        | 0.241        | 0.402        | 0.135        | 0.232        | 0.416        | 0.552        | 0.269        | 0.291        | <b>0.820</b> | 0            | 0            | 0            | 0            | 0            |
| PP  | 0.166        | 0.395        | 0.013        | -0.117       | 0.038        | 0.121        | 0.116        | 0.035        | 0.037        | 0.206        | <b>0.810</b> | 0            | 0            | 0            | 0            |
| PS  | 0.335        | 0.331        | 0.263        | 0.014        | 0.077        | 0.277        | 0.222        | 0.076        | 0.118        | 0.413        | 0.339        | <b>0.865</b> | 0            | 0            | 0            |
| PU  | 0.654        | 0.019        | 0.410        | 0.207        | 0.459        | 0.405        | 0.352        | 0.496        | 0.460        | 0.472        | 0.168        | 0.316        | <b>0.821</b> | 0            | 0            |
| SE  | 0.449        | -0.038       | 0.394        | 0.431        | 0.726        | 0.357        | 0.335        | 0.658        | 0.672        | 0.326        | 0.069        | 0.168        | 0.489        | <b>0.807</b> | 0            |
| SN  | 0.527        | 0.149        | 0.402        | 0.159        | 0.311        | 0.400        | 0.514        | 0.360        | 0.294        | 0.718        | 0.163        | 0.322        | 0.536        | 0.372        | <b>0.829</b> |

In conclusion, except for BEH6, BEH7, and BEH8 that have low values of factor loading, the rest of the instruments demonstrate satisfactory reliability and validity.

**Hypotheses testing.** This study utilized the Structural Equation Modeling (SEM), specifically Smart PLS to examine each hypothesis. Gefen, Straub and Boudreau (2000) state the casual relations and qualitative assumptions can be analyzed and estimated utilizing Structural Equation Modeling. The major strength of SEM is constructing latent variables.

The SmartPLS utilizes the Partial Least Squares (PLS) method for latent variables analysis. Not only could the SmartPLS be used to examine factors loading and reliability testing, but it could also be used to construct the path coefficient table including T-test values; and visualizing the latent variables. According to Gefen, Straub and Boudreau (2000), "SEM has become *de rigueur* in validating instruments and testing linkages between constructs" (p. 6). The smartPLS calculate the T-statistics for significance testing of both the inner and outer model, using a procedure called bootstrapping. In this procedure the software takes a large number of subsamples from the original sample with replacement to give bootstrap standard errors, which in turn gives approximated T-value for significance testing of the structural path. Also, the Bootstrap result approximates the normality of data (Wong, 2013, p. 23). According to Wong (2013), "Using a two-tailed T-test with a significance level of 5% the path coefficient will be significant if the T-statistic is larger than 1.96" (p. 24). Since the developed research model in this study is reflective, the following analyses are required: explanation of target endogenous variable variance, inner model path coefficient sizes and significance, and structural path significance.

**Explanation of target endogenous variable variance.** Figure 12 illustrated the results

of the standard PLS procedure, which calculate the path modeling and effect of the other latent variables on specific variables by SmartPLS. As demonstrated in Figure 12, each construct has been modeled with a circle and path coefficients have been placed on the arrow between variables. The number inside the circles is a coefficient of determinations, Rsquare, which shows how much the variance of the latent variable is being explained by the other latent variables. For example, the coefficient of determination, Rsquare, for the attitude (ATT) latent variable is 0.451. This means that 45.1 % variance in ATT has been explained by four latent variables of PP, PS, PU, and PEU.

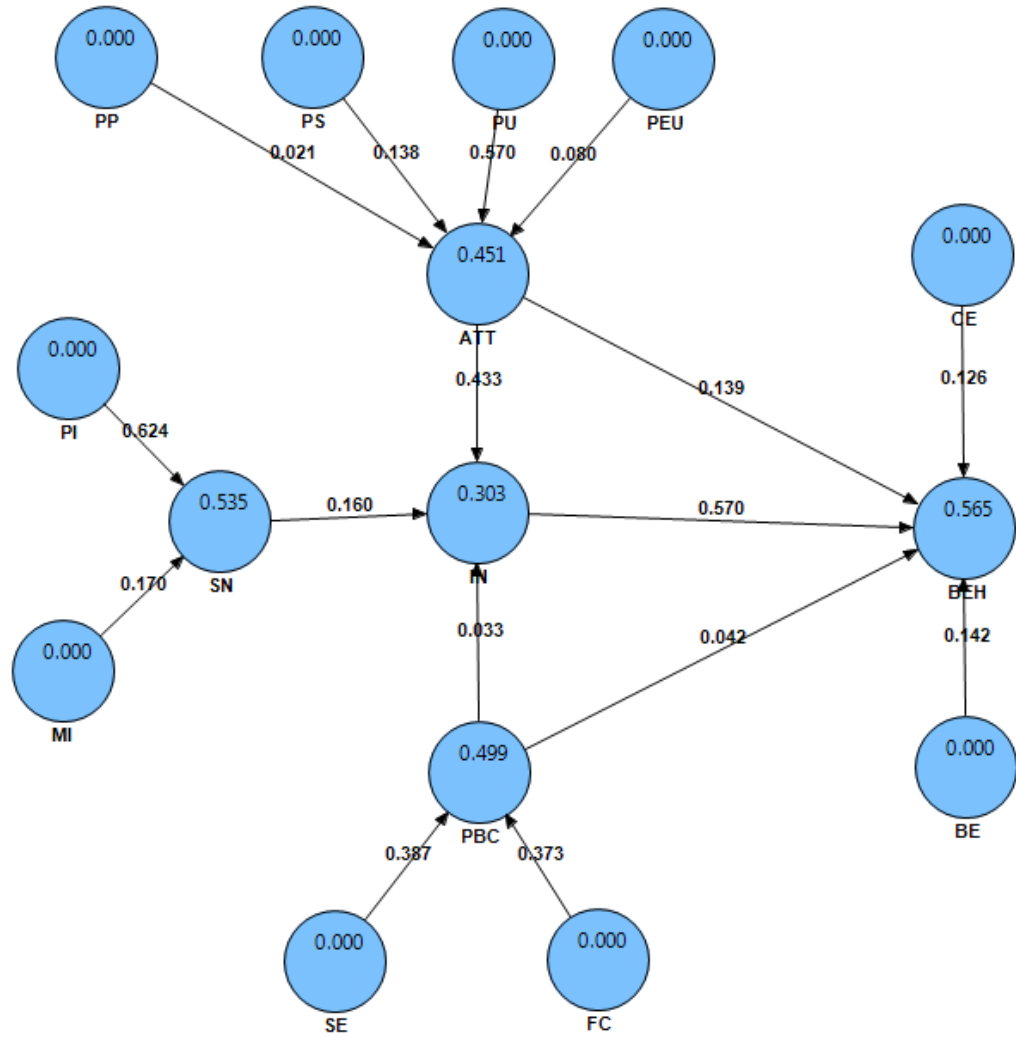


Figure 12. SmartPLS path modeling results

Table 11 summarizes the results of the explanation of target endogenous variable variance achieved from SmartPLS standard path coefficient analysis.

Table 11

*Explanation of Variable Variance Analysis*

| <b>Latent variable</b>              | <b>Explanation of target endogenous variable variance</b>   |
|-------------------------------------|---|
| <b>Attitude</b>                     | 45.1% of the variance in Attitude (ATT) has been explained by the variables of PP, PS, PU, and PEU.           |
| <b>Subjective Norm</b>              | 53.5% of the variance in Subjective Norm (SN) has been explained by the variables of PI and MI.               |
| <b>Perceived Behavioral Control</b> | 49.9% of the variance in Perceived Behavioral Control (PBC) has been explained by the variables of SE and FC. |
| <b>Intention</b>                    | 30.3% of the variance in Intention (IN) has been explained by ATT, SN, and PBC.                               |
| <b>Behavior</b>                     | 56.5% of the variance in Behavior (BEH) has been explained by ATT, IN, PBC, CE, and BE.                       |

**Inner model path coefficient sizes and significance.** The second groups of numbers that have been demonstrated in Figure 13 are inner model path coefficients, which are placed on the arrows between the variables. According to Wong (2013), the standardized path coefficient value larger than 0.1 is a strong predictor of the corresponding latent variables. For instance, the standardized path coefficient value between perceived probability (PP) and attitude (ATT) is 0.021, which is smaller than 0.1. For this reason, the hypothesized path relationship between PP and ATT is not statistically significant. On the other hand, since the inner path coefficient between perceived severity (PS) and attitude (ATT) is 0.138 and larger than 0.1, we can conclude that the hypothesized path relationship between PS and ATT is statistically significant. Table 12 summarizes the results of the inner model path coefficient sizes and significance.

Table 12

*Inner Model Path Coefficient Sizes and Significance*

| <b>Latent variable</b> | <b>Inner Model Path coefficient sizes and significance</b>  |
|------------------------|---|
| ATT                    | <ul style="list-style-type: none"> <li>• The hypothesized path relationship size between PP and ATT is 0.021, so it is not statistically significant.</li> <li>• The hypothesized path relationship size between PS and ATT is 0.138, so it is statistically significant.</li> <li>• The hypothesized path relationship size between PU and ATT is 0.570, so it is statistically significant.</li> <li>• The hypothesized path relationship size between PEU and ATT is 0.080, so it is not statistically significant.</li> </ul> |
| SN                     | <ul style="list-style-type: none"> <li>• The hypothesized path relationship size between PI and SN is 0.624, so it is statistically significant.</li> <li>• The hypothesized path relationship size between MI and SN is 0.170, so it is statistically significant.</li> </ul>  |
| PBC                    | <ul style="list-style-type: none"> <li>• The hypothesized path relationship size between FC and PBC is 0.373, so it is statistically significant.</li> <li>• The hypothesized path relationship size between SE and PBC is 0.387, so it is statistically significant.</li> </ul>  |
| IN                     | <ul style="list-style-type: none"> <li>• The hypothesized path relationship size between ATT and IN is 0.433, so it is statistically significant.</li> <li>• The hypothesized path relationship size between SN and IN is 0.160, so it is statistically significant.</li> <li>• The hypothesized path relationship size between PBC and IN is 0.033, so it is not statistically significant.</li> </ul>   |
| BEH                    | <ul style="list-style-type: none"> <li>• The hypothesized path relationship size between ATT and BEH is 0.139, so it is statistically significant.</li> <li>• The hypothesized path relationship size between IN and BEH is 0.627, so it is statistically significant.</li> <li>• The hypothesized path relationship size between PBC and BEH is 0.058,</li> </ul>  |



|  |   |
|--|---|
|  | <p>so it is not statistically significant.</p> <ul style="list-style-type: none"> <li>• The hypothesized path relationship size between CE and BEH is 0.126, so it is statistically significant.</li> <li>• The hypothesized path relationship size between BE and BEH is 0.142, so it is statistically significant.</li> </ul> |
|--|---|

In summary except the following inner path coefficient of: PP and ATT (0.021); PEU and ATT (0.080); PBC and IN (0.033); and PBC and BEH (0.058), the rest of the hypothesized path relationships are statistically significant. In the next step to examine the research hypotheses this study utilized the Bootstrapping procedure in SmartPLS.

**Checking structural path significance in bootstrapping.** Another important procedure that has been used through SmartPLS to generate the T-statistic for significance testing of a given research hypotheses is Bootstrapping. According to Wong (2013), using a two-tailed T-test with a significance level of 5% the path coefficient will be significant if the T-statistic is larger than 1.96 (p. 24). Also, Weaver (2011), stated that, any score greater than -2 or +2 is acceptable and satisfactory to approve a corresponding hypothesis. Table 13 presents the path coefficient and t-values achieved using the Bootstrapping procedure along with the results of the hypotheses testing.

Table 13

*Hypothesis Testing*

| <b>Row</b> | <b>Path</b>   | <b>Hypothesis</b> | <b>Path Coefficient</b> | <b>t-value</b> | <b>Result</b> |
|------------|---|-------------------|-------------------------|----------------|---------------|
| 1          | Perceived Ease of Use (PEU) → Security Attitude (ATT)           | H1a               | 0.080                   | 1.774          | Rejected      |
| 2          | Perceived Usefulness (PU) → Security Attitude (ATT)             | H1b               | 0.570                   | 11.2421        | Accepted      |
| 3          | Perceived Severity (PS) → Security Attitude (ATT)               | H1c               | 0.138                   | 3.3178         | Accepted      |
| 4          | Perceived Probability (PP) → Security Attitude (ATT)            | H1d               | 0.021                   | 0.6477         | Rejected      |
| 5          | People's Influence (PI) → Subjective Norm(SN)                   | H2a               | 0.624                   | 19.2036        | Accepted      |
| 6          | Media's Influence (MI) → Subjective Norm (SN)                   | H2b               | 0.170                   | 4.5069         | Accepted      |
| 7          | Facilitating Condition (FC) → Perceived Behavioral Control(PBC) | H3a               | 0.373                   | 6.5895         | Accepted      |
| 8          | Self-Efficacy (SE) → Perceived Behavioral Control(PBC)          | H3b               | 0.387                   | 6.8198         | Accepted      |
| 9          | Security Attitude (ATT) → Security Intention (IN)               | H4a               | 0.433                   | 10.2636        | Accepted      |
| 10         | Subjective Norm (SN) → Security Intention (IN)                  | H4b               | 0.160                   | 3.7865         | Accepted      |
| 11         | Perceived Behavioral Control(PBC) → Security Intention (IN)     | H4c               | 0.033                   | 0.801          | Rejected      |

|    |   |     |       |         |          |
|----|---|-----|-------|---------|----------|
| 12 | Security Attitude (ATT)<br>→ Security Behavior<br>(BEH)             | H5a | 0.139 | 3.6392  | Accepted |
| 13 | Security Intention (IN)<br>→ Security Behavior<br>(BEH)             | H5b | 0.627 | 12.6785 | Accepted |
| 14 | Perceived Behavioral<br>Control(PBC)<br>→Security Behavior<br>(BEH) | H5c | 0.058 | 1.4069  | Rejected |
| 15 | Computing Experience<br>(CE) →Security<br>Behavior (BEH)            | H5d | 0.126 | 4.0585  | Accepted |
| 16 | Breach Experience (BE)<br>→Security Behavior<br>(BEH)               | H5e | 0.142 | 4.0368  | Accepted |

- Hypothesis 1

H1a: There is a positive relationship between users' perceived ease of use of and security attitude to practice security behaviors in smartphones.

The results of the PLS-SEM from Bootstrapping analysis reveals that the T-statistics between PEU and ATT is 1.7748, which is smaller than 1.96. For this reason there is no significant relationship between smartphone users' perceived ease of use (PEU) and users' security attitude (ATT) toward utilizing security technologies in smartphones. Moreover, this conclusion confirms the previous finding regarding the path coefficient of 0.080, which shows there is no statistical significance relationship between PEU and ATT. For these reasons, this hypothesis has been rejected.

- Hypothesis 2

H1b: There is a positive relationship between users' perceived usefulness (PU) and security attitude (ATT) to practice security behavior in smartphones.

The SEM result reveals that there is a significant positive relationship between users' usefulness perception of utilizing security technology and their attitude toward utilizing these technologies on smartphones. This hypothesis has been accepted because the t-value is 11.2421 and larger than 1.97. This conclusion also has been confirmed by the path coefficient of 0.570.

- Hypothesis 3

H1c: There is a positive relationship between users' perceived severity (PS) of security breaches and attitude (ATT) to practice security behavior in smartphones.

According to the SEM results in Table 13 the tow-statistics value is equal 3.178, which is a satisfactory (larger than 1.96) indicator to accept the hypothesis. Also, such a relationship has been confirmed by path coefficient value of 0.138, which is larger than 0.1 and great indication of significant relationship between PS and ATT.

- Hypothesis 4

H1d: There is a positive relationship between users' perceived probability (PP) of security breaches and attitude (ATT) to practice security behavior in smartphones.

The results of the SEM calculated utilizing SmartPLS shows that t-value for the relationship between PP and ATT is equal to 0.6477, which is smaller than 1.96. Also, the value of path coefficient, 0.021, is smaller than 0.1. For these reasons this hypothesis is rejected. In another word, there is no statistical significant relationship between PP and ATT.

- Hypothesis 5

H2a: There is a positive relationship between people's influence (PI) and subjective norm (SN) to practice security behavior in smartphones.

This hypothesis is accepted because the t-value resulted through SEM, 19.2036, is higher than 1.96 and the path coefficient, 0.624, is larger than 0.1. For all of these reasons, this study concludes that there is strong positive relationship between people's influence (PI) and subjective norm (SN).

- Hypothesis 6

H2b: There is a positive relationship between users' media's influence (MI) and subjective norm (SN) to practice security behavior in smartphones.

The SEM results presented in Table 13 reveal that there is a significant positive relationship between media's influence and subjective norm. This hypothesis has been approved because the t-value (4.5069) meets the threshold for the p-value of 0.05. Also, the same conclusion could be confirmed through the results of the path coefficient (0.624) which is above the threshold of 0.1, which is great indicator of significant statistical relationship between MI and SN.

- Hypothesis 7

H3a: There is a positive relationship between users' facilitating conditions (FC) and perceived behavioral control (PBC) to practice security behavior in smartphones.

According to the results of the SEM, there is a positive significant relationship between FC and PBC. The path coefficient (0.373) is above

acceptable threshold of 0.1 which confirm a significant relationship between the hypothesized path of FC and PBC. Also, this hypothesis has been accepted because the t-value (6.5895) is above the threshold value of 1.96 and p-value of 0.05.

- Hypothesis 8

H3b: There is a positive relationship between users' self-efficacy (SE) and perceived behavioral control (PBC) to practice security behavior in smartphones.

The results of the SEM reveal that there is a significant positive relationship between self-efficacy (SE) and perceived behavioral control (PBC). The significant relationship between SE and PBC initially has suspected by the value of path coefficient (0.387), which is above 0.1. Later this hypothesis has been confirmed and accepted because the t-value (6.8198) meets the threshold for the p-value of 0.05.

- Hypothesis 9

H4a: There is a positive relationship between users' attitude (ATT) and intention (IN) to practice security behavior in smartphones.

This hypothesis has been approved because the t-value (10.2636) meets the threshold for the p-value of 0.05. In conclusion, smartphone users' attitude toward security technologies has a positive and significant impact on their intention toward using these security technologies.

- Hypothesis 10

H4b: There is a positive relationship between users' subjective norm (SN) and intention (IN) to practice security behavior in smartphones.

The analysis of SEM utilizing SmartPLS reveals that there is a positive relationship between smartphone's subjective norm and their intention toward using security technology in smartphones. The hypothesized path relationship between SN and IN has been suspected initially by analyzing the path coefficient (0.160), which is above the threshold of 0.1. Finally the hypothesis has been accepted because the t-value (3.7865) is above 1.96 and meets the threshold for the p-value of 0.05.

- Hypothesis 11

H4c: There is a positive relationship between users' perceived behavioral control (PBC) and intention (IN) to practice security behavior in smartphones.

The results of the PLS-SEM show that there is no significant relationship between perceived behavioral control and intention in the selected sample size. This hypothesis has been rejected because the t-value (0.801) does not meet the threshold for two-tailed statistical p-value of the 0.05. Also, the value of the path coefficient (0.033) does not meet the threshold value of 0.1 and confirm the rejection of this hypothesis.

- Hypothesis 12

H5a: There is a positive relationship between users' attitude (ATT) and practicing security behavior (BEH) in smartphones.

According to the results of the SEM demonstrated in Table 13 there is significant positive relationship between users' attitude toward using security technologies in smartphones and their actual security behavior. This hypothesis has been accepted because the t-value (3.6392) is larger than 1.96 and meet the threshold for the p-value of 0.05. Also, the value of path coefficient (0.139) confirms the significant relationship between ATT and BEH.

- Hypothesis 13

H5b: There is a positive relationship between users' intention (IN) and practicing security behavior (BEH) in smartphones.

The results of the PLS-SEM derived from SmartPLS in Table 13 confirm that there is a significant positive relationship between users' attitude toward using security technologies in smartphone and their actual adaptation of security technology. Initially, the path coefficient (0.627) reveals the strong relationship between IN and BEH and finally, the t-value (12.6785), which is larger than 1.96 and meets the threshold for p-value of 0.05, confirms the hypothesis.

- Hypothesis 14

H5c: There is a positive relationship between users' perceived behavioral control and practicing security behavior in smartphones.

The result of the SEM analysis on the selected sample size does not show any significant relationship between perceived behavioral control and actual adaptation of security technologies in smartphones. This hypothesis has been rejected because the path coefficient (0.058) is lower than critical value



0.1 and the t-value (1.4069) does not meet the threshold for the p-value of 0.05.

- Hypothesis 15

H2a: There is a positive relationship between users' Computing Experience (CE) and practicing security behavior (BEH) in smartphones.

This hypothesis is accepted because the t-value resulted through SEM analysis, 4.0585, is higher than 1.96 and the path coefficient, 0.126, is larger than 0.1. For all of these reasons, this study concludes that there is strong positive relationship between Computing Experience (CE) and practicing security behavior (BEH).

- Hypothesis 16

H3a: There is a positive relationship between users' Breach Experience (BE) and practicing security behavior (BEH) in smartphones.

According to the results of the SEM analysis, there is a positive significant relationship between BE and BEH. The path coefficient (0.142) is above acceptable threshold of 0.1 which confirm a significant relationship between the hypothesized path of FC and PBC. Also, this hypothesis has been accepted because the t-value (4.0368) is above the threshold value of 1.96 and meets the threshold for the p-value of 0.05.

**Moderating factors.** If an independent variable could change the direction or the strength of the relationship between two constructs, that variable has a moderation impact. This study has chosen gender and employment status as independent variables to test their moderation effects on the hypothesized paths in the research model.

To find the effects of the gender this study filtered and created two different datasets for males and females and then executed a PLS-SEM statistical analysis. The male group had 325 records, which represented of 54.8% of the sample size, and the female group had 268 records, which represented the 45.2% of the sample size. Table 14 presents the results of the SEM for the two groups of male and female.

Table 14

*PLS-SEM Analysis for Two Groups of Male and Female*

| Hypothesis     | t-value,<br>overall | t-value,<br>Male | t-value,<br>Female | Moderation effect |
|----------------|---------------------|------------------|--------------------|-------------------|
| H1a. PEU → ATT | 1.7673              | 0.2525           | 2.3707             | Yes               |
| H1b. PU → ATT  | 11.0325             | 10.0634          | 5.5649             | No                |
| H1c. PS → ATT  | 3.0392              | 2.0221           | 3.0651             | No                |
| H1d. PP → ATT  | 0.6304              | 0.6746           | 0.6522             | No                |
| H2a. PI → SN   | 18.8488             | 12.6785          | 14.1403            | No                |
| H2b. MI → SN   | 4.4228              | 3.9821           | 1.9765             | No                |
| H3a. FC → PBC  | 6.2993              | 4.4847           | 5.4455             | No                |
| H3b. SE → PBC  | 6.4991              | 5.4215           | 5.1189             | No                |
| H4a. ATT → IN  | 11.1975             | 7.8929           | 6.8029             | No                |
| H4b. SN → IN   | 3.5512              | 2.1202           | 2.7142             | No                |

|                |         |         |        |     |
|----------------|---------|---------|--------|-----|
| H4c. PBC → IN  | 0.8858  | 0.4815  | 1.4903 | No  |
| H5a. ATT → BEH | 3.4311  | 1.8037  | 3.3645 | Yes |
| H5b. IN → BEH  | 12.1396 | 11.3532 | 7.936  | No  |
| H5c. PBC → BEH | 1.4161  | 1.294   | 0.5748 | No  |
| H5d. CE → BEH  | 4.2075  | 2.2032  | 2.9455 | No  |
| H5e. BE → BEH  | 3.8113  | 3.8511  | 2.3064 | No  |

As illustrated in Table 14, the female group shows strong relationships in two hypothesized paths of “H1a” (PEU → ATT) and “H5a” (ATT → BEH). The t-values in hypothesized paths of H1a (2.3707) and H5a (3.3645) for the female group is above the threshold value of 1.96 and meets the required p-value of 0.05, while the male group does not meet the threshold for the p-value and does not show any strong significant relationship. For these reasons, gender moderated the relationship between PEU and ATT; and ATT and BEH. Moreover, the SEM analysis displayed in Table 14 reveals that gender doesn’t moderate other hypothesized paths.

To examine the impact of employment status, this research has filtered the respondents who claim to be employed in one group and the remaining records from the unemployed group. The employed group had 415, which represented 70% of the sample size, and the unemployment group had 178 members, which presenting 30% of the study’s sample size. Table 15 illustrates the results of the PLS-SEM analysis of the employed and

unemployed group. Also, this table shows if employment has a moderating effect on any of the hypothesized paths.

Table 15

*PLS-SEM Analysis for Two Groups of Employed and Unemployed*

| <b>Hypothesis</b> | <b>t-value,<br/>overall</b> | <b>t-value,<br/>Employed</b> | <b>t-value,<br/>Unemployed</b> | <b>Moderation<br/>effect</b> |
|-------------------|-----------------------------|------------------------------|--------------------------------|------------------------------|
| H1a. PEU → ATT    | 1.7673                      | 1.7897                       | 0.8178                         | No                           |
| H1b. PU → ATT     | 11.0325                     | 12.6931                      | 4.374                          | No                           |
| H1c. PS → ATT     | 3.0392                      | 2.0976                       | 2.8459                         | No                           |
| H1d. PP → ATT     | 0.6304                      | 1.0474                       | 0.3479                         | No                           |
| H2a. PI → SN      | 18.8488                     | 15.3692                      | 14.6244                        | No                           |
| H2b. MI → SN      | 4.4228                      | 3.1272                       | 3.4967                         | No                           |
| H3a. FC → PBC     | 6.2993                      | 9.362                        | 1.1298                         | Yes                          |
| H3b. SE → PBC     | 6.4991                      | 4.5708                       | 8.2609                         | No                           |
| H4a. ATT → IN     | 11.1975                     | 7.901                        | 6.556                          | No                           |
| H4b. SN → IN      | 3.5512                      | 3.0616                       | 1.8391                         | Yes                          |
| H4c. PBC → IN     | 0.8858                      | 0.3864                       | 0.7171                         | No                           |
| H5a. ATT → BEH    | 3.4311                      | 2.5205                       | 2.2216                         | No                           |

|                |         |         |        |     |
|----------------|---------|---------|--------|-----|
| H5b. IN → BEH  | 12.1396 | 11.8155 | 7.1716 | No  |
| H5c. PBC → BEH | 1.4161  | 1.2631  | 0.378  | No  |
| H5d. CE → BEH  | 4.2075  | 3.8548  | 1.6729 | Yes |
| H5e. BE → BEH  | 3.8113  | 3.7526  | 2.2679 | No  |

According to the results of the SEM for both groups of the employed and unemployed users, the following relationships have been moderated by the employment status:

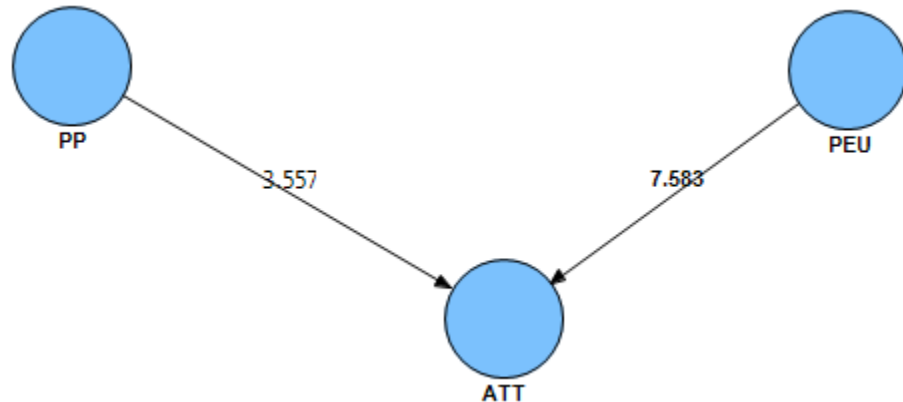
In the hypotheses of H3a, the t-value for the employed group meets the requirement for the p-value threshold of 0.05 and the t-value is larger than 1.96. For this reason in the employed group the FC had a significant positive relationship with PBC. On the other hand, the FC did not have a significant relationship with PBC in the unemployed group.

Since the t-value in the employed group is 3.016, the hypotheses of H4b (SN → IN) was accepted in the employed group, while the same hypothesis was rejected in the unemployed group. In other words, the relationship between users' Subjective Norm (SN) and security intention (IN) in smartphones was moderated by the employment status of the respondents in this study.

Finally, hypothesis H5d, (CE → BEH) was moderated by employment status. As illustrated in Table 15, the t-value of this hypothesis for the employed group met the threshold for t-value, while the t-value for the unemployed group was lower than 1.96.

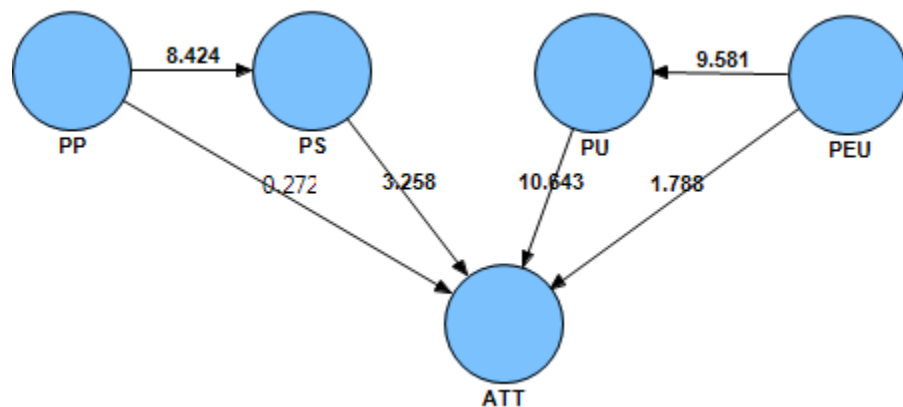
**Mediating factors.** A mediating factor is a variable or construct that could intervene between two other related constructs. According to Hair, Sarstedt, Ringle, and Mena (2012), one of the main applications of mediation is to explain why a relationship between two

construct exists. This study examined the mediation effect of perceived severity (PS) and perceived usefulness (PU) on two hypotheses of H1a (PEU  $\rightarrow$  ATT) and H1d (PP  $\rightarrow$  ATT). Figure 13 displays the results of Bootstrapping in SmartPLS-SEM for the two hypotheses of H1a and H1d without mediation factors of PU and PS. As illustrated in Figure 13, t-values for both hypotheses, located on the arrows between constructs, are larger than 1.96.



*Figure 13.* Analysis of SEM without mediating factors

In order to examine the mediation effect of PU and PS, the following model (Figure 14) was created and tested. As presented in Figure 14, although the t-value between each independent variable and mediator was satisfactory but the t-value in the main hypothesized paths of H1a and H1d were not significant (smaller than 1.96).



*Figure 14.* Analysis of SEM with mediating factors

In conclusion, as presented in Table 16, perceived severity (PS) mediated the relationship between perceived probability (PP) and users' security attitude (ATT); and perceived severity (PS) mediates the relationship between perceived ease of use (PEU) and users' security attitude (ATT).

Table 16

*Mediation Factors*

| <b>Hypothesis</b> | <b>Mediator</b> | <b>t-value,<br/>without<br/>mediator</b> | <b>t-value, with<br/>mediator</b> | <b>Mediation<br/>effect</b> |
|-------------------|-----------------|--|-----------------------------------|-----------------------------|
| H1a. PEU → ATT    | PU              | 7.583                                    | 0.272                             | Yes                         |
| H1d. PP → ATT     | PS              | 3.557                                    | 1.788                             | Yes                         |

**Summary**

This study had used applications such as Microsoft Excel, SPSS, and SmartPLS to analyze the collected data including completed rate, demographic characteristics, reliability, normality, validity, hypothesis test, and moderators' effects. Cronbach's Alpha coefficients along with composite reliability were used to estimate the reliability and internal consistency of the developed instrument. The data normality was assessed using Skewness and Kurtosis calculations. Moreover, this study performed confirmatory factor analysis to ensure that all the items with a specific construct highly correlated with each other and they addressed the main constructs. The results of this analysis reveal that only BEH6, BEH7, and BEH8 could

not load in the construct of security behavior (BEH). For this reason this study eliminates these items from the rest of the analysis.

Construct validity was tested using content validity, convergent validity and discriminant validity. The results of these tests demonstrate high construct validity and ensure the validity of the survey.

Structural Equation Modeling analysis performed in SmartPLS has used to assess the research hypothesis. An analysis of the data revealed that hypotheses H1a (PEU  $\rightarrow$  ATT), H1d (PP  $\rightarrow$  ATT), H4c (PBC  $\rightarrow$  IN), and H5c (PBC  $\rightarrow$  BEH) were rejected, while hypotheses H1b, H1c, H2a, H2b, H3a, H3b, H4a, H4b, H5a, and H5b were accepted.

This study examined the impact of gender and employment status as moderators on the hypothesized paths. The analysis of SEM for two groups of male and females shows that the gender plays a moderating role for two hypothesized paths of “H1a” (PEU  $\rightarrow$  ATT) and “H5a” (ATT  $\rightarrow$  BEH). Also, the analysis of SEM for the two groups of employed and unemployed revealed that employment played a moderating role for three hypothesized paths of “H3a” (FC  $\rightarrow$  PBC), “H4b” (SN  $\rightarrow$  IN), and “H5d” (CE  $\rightarrow$  BEH). These findings and their implication will be discussed in Chapter 5.

Finally, this study tested the mediation effects of PU and PS on the two hypotheses of H1a and H1d. The results of the SEM analysis showed that PU mediated the relationship between PEU and ATT; and PS mediated the relationship between PP and ATT.



## **Chapter 5. Discussion, Conclusions, and Implications**

This chapter is divided into the following sections: overview of the study, discussion of the findings; analysis of research conclusions; implications of the study's results; limitations of the research; and recommendations for future research.

### **Overview of the Study**

This study attempted to assess users' information security behavior in smartphone networks. A thorough review of the literature identified appropriate theoretical models to identify and examine the variables that could possibly affect users' behavior toward adoption or rejection of information security behavior in smartphones. From all the factors that might affect behavior, this study focused on the following factors: security behavior, security intention, security attribute, perceived behavioral control, perceived ease of use, perceived usefulness, perceived severity, perceived probability, people's influence, media's influence, self-efficacy, and facilitating conditions. Based on the selected variables and the literature, this study formed a research model and utilized an investigator-developed survey questionnaire to examine the theoretically-based hypothesized paths. The research adapted both convenient and snowball sampling to increase the number of usable research responses. The study was conducted at Eastern Michigan University (EMU) in Ypsilanti, Michigan. By posting the survey on EMU's online daily announcements, EMU's Facebook page, and several classes at EMU's College of Technology, the study obtained a sample size of 593 participants. Finally, this research utilized statistical analysis software including Microsoft Excel, SPSS, and SmartPLS to perform statistical analyses.

**Discussion**

This research tested 16 hypotheses to assess the factors that might affect users' behavior toward adoption of security technology in smartphones. As shown in Figure 15, the PLS-SEM analysis revealed that four hypotheses were rejected and the remaining twelve hypotheses were accepted.

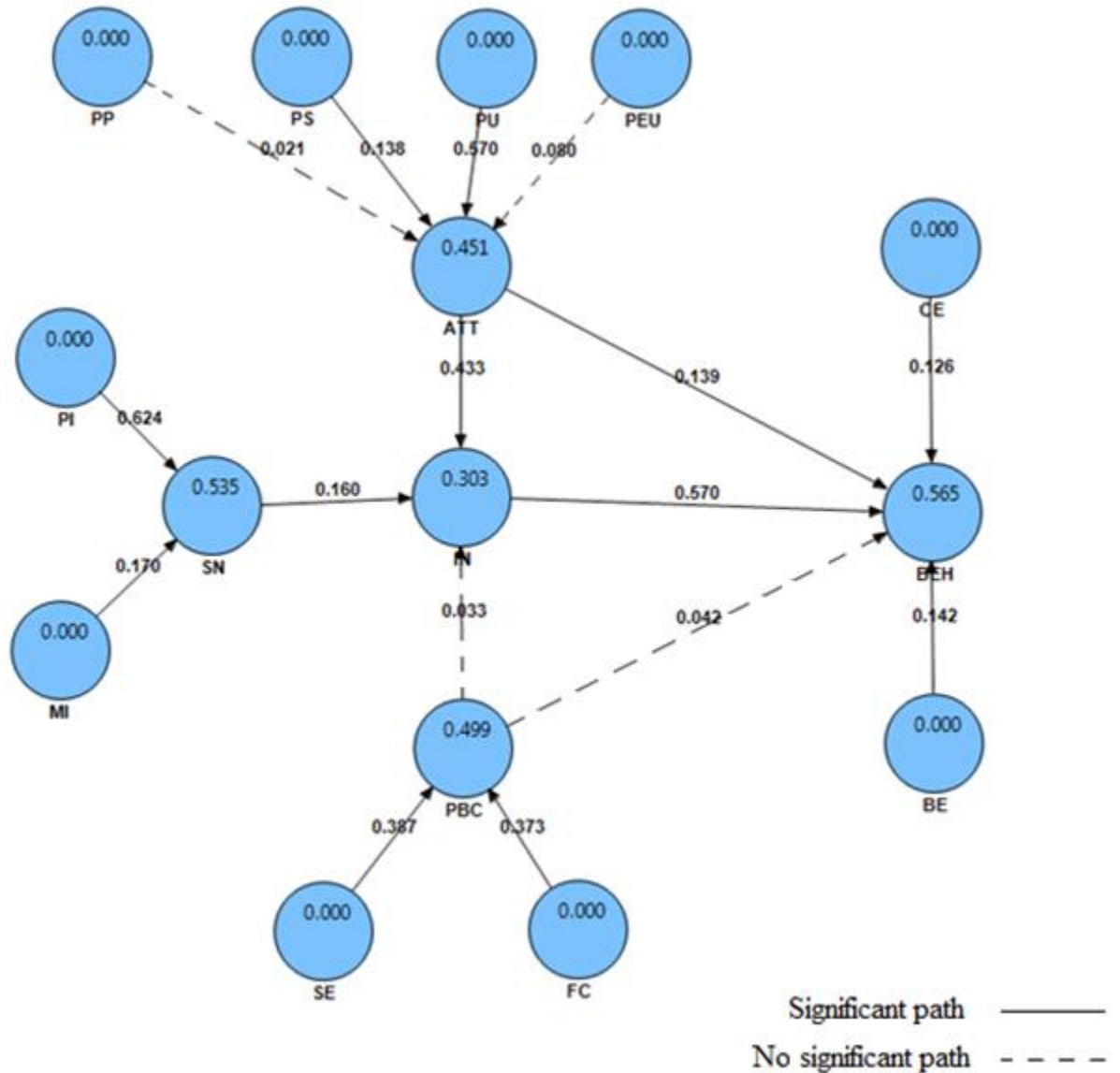


Figure 15. Results of PLS-SEM path analysis

This study revealed that users' attitude toward the adoption of security technology was affected primarily by their perception of a possible security breach severity and their perceptions toward the usefulness of these security technologies. If the users thought that the security breaches would affect them severely, and/or if they believed that using the security technologies on their smartphones would be useful, then they tended to have more positive attitudes about using these technologies on their smartphones.

In contrast, this study found no significant relationship between users' perception of ease of use or probability of a security breach and their attitudes toward using this security technology on their smartphones. Although the initial analysis did not find statistical significance between users' perception of ease of use and their attitude, the analysis of moderators altered that finding. Analyzing the effect of moderators, this study found females' (but not males') perception of ease of use directly affected their attitude toward utilizing security technologies in smartphones. Additionally, the same analysis showed that the male users' security attitude did not have a significant relationship with intention. If the users were employed, their facilitation condition (FC) had a significant positive relationship with their perceived behavioral control (PBC). The employed users of smartphones believe that available resources are a key component in their sense of control over their behaviors. The moderating effect of employment on the relationship between subjective norms and intention also showed the importance of societal pressures (from peers, coworkers, managers, etc...) on the intention to adapt security technology on the employed group. This also could suggest that society's pressures are less effective on jobless respondents. The subjective norm factors of people's and media's influences also affected users' perceived social pressure toward utilizing security technologies in smartphones.

Users' self-efficacy and facilitating condition positively affected their perceived behavioral controls. If the users believed they could perform a behavior and they could have access to any required hardware and firmware, it positively affected their perceptions toward having control over their behavior and its consequences.

This study defined the security intention as users' desire to adapt security technology in smartphones. This research examined the effects of users' security attitudes, subjective norms, and perceived behavior controls on their intentions to adapt security technologies in smartphones. The analyses of PLS-SEM revealed that users' security behaviors and users' subjective norms influenced their intentions to adapt security behaviors. If smartphone users had a positive attitude toward using security technologies and perceived pressure from influential people, they were more willing to change their intentions to use these technologies. The analysis of moderator effects revealed that gender also played an important role in the relationship between perceived behavioral control and users' security intention; i.e. perceived behavioral control significantly affected female users' security intention but this hypothesized path was not significant among male users. Although intention examined users' *desire* to use security technologies, it did not mean they adopted these behaviors.

To examine users' actual security behavior, this study formed another construct and hypothesized that there are positive significant relationships between security attitudes, security intentions, and perceived behavioral controls. From these hypotheses, the analyses only found that the security attitudes and intentions had significant relations with security behavior while perceived behavioral control had no significant relationship with security behavior. It could be concluded that if the users had positive attitudes toward the adoption of security technologies and had positive intentions to use these technologies, they would be

more willing to actually adopt these technologies. The analysis of moderators revealed, in contrast to the unemployed users, there was a significant positive relationship between users' computing experience and users' security behavior among employed members.

### **Research Conclusions**

In this study, five research questions were addressed. These questions and the obtained results are discussed as follows:

#### Research Question 1

1. *"What are the factors that might affect users' attitudes toward practicing various security behaviors in the domain of smartphone networks?"*

This study identified four possible factors of perceived ease of use, perceived usefulness, perceived severity of threat, and perceived probability that might affect users' security attitudes. This study formed and examined four hypotheses.

In the first hypothesis (H1a), assessment of the relationship between perceived ease of use and security attitudes, this study's finding did not confirm the results of Park and Chen (2007). However, analyzing the impacts of the moderators on this hypothesized path showed that this hypothesis was accepted among female respondents or employed users.

In the second hypothesis (H1b), the significant relationship between perceived usefulness and users' security attitude was approved and confirmed the results of the previous studies (Ng & Rahim, 2005; Park & Chen, 2007; Taylor & Todd, 1995c). In the third hypothesis (H1c), the positive significant relationship between perceived probability and users' security attitudes was accepted and was similar to the study's findings which confirmed the results given by Herath and Rao (2009).

The fourth hypothesis (H1c), the assessment of the relationship between the perceived severity and users' security attitude, was rejected and did not confirm the findings by Herath and Rao (2009). This discovery indicated that users' attitudes toward the adoption of security technologies in smartphones were not affected by their perceived severity of security breach incidents on their devices.

#### Research Question 2

2. *“What are the factors that might affect subjective norms on users in smartphone networks?”*

This research selected two important factors: people and the media as social influencers on the users' behavior toward the adoption of security technologies in smartphones. This study formed and tested two hypotheses.

In the first hypothesis (H2a), a significant relationship was found between peoples' influence and subject norms, which confirmed the findings reported by Ajzen (1988, 1991), Herath and Rao (2009), and Ng and Rahim (2005). In hypothesis (H2b), the relationship between media's influence and users' subjective norms, accepted and confirmed the results of the study by Ng and Rahim (2005). These findings revealed that social pressure on a user, known as the subjective norm, was indeed affected by influential people as well as by the media.

#### Research Question 3

3. *“What are the factors that might affect users' perceived behavioral control?”*

Perceived behavioral control was modeled utilizing two main factors: facilitating condition and self-efficacy. The research analysis demonstrated a significant relationship between the selected factors and perceived behavioral control. The

hypotheses of H3a and H3b were accepted and confirmed the findings reported by Ng and Rahim (2005), and Park and Chen (2007).

#### Research Question 4

4. *“What are the factors that might affect users’ intentions toward practicing security behavior in smartphones?”*

This study hypothesized three factors that could affect users’ security intention: security attitudes, subjective norms, and perceived behavioral controls. The first hypothesis (H4a), the relationship between users’ security attitudes and security intentions, was significant and confirmed similar findings in previous studies such as Ng and Rahim (2005) and Park and Chen (2007).

The second hypothesis (H4b), assessment of the relationship between subjective norms and users’ security intentions, accepted and confirmed the results of the studies by Ng and Rahim (2005) and Ajzen (1988, 1991).

The third hypothesis (H4c), which focused on the impacts of perceived behavioral control on users’ security intention, was rejected. This finding confirmed the results of the Decomposed Theory of Planned Behavior examined by Ng and Rahim (2005).

#### Research Question 5

5. *“What are the factors that might affect users’ practicing security behavior in smartphones?”*

The possible influential factors that could affect users’ adoption of security technology in smartphone usage included to users’ security attitude, users’ security

intention, and users' perceived behavioral control. Three hypotheses were tested to examine these relationships.

The first hypothesis (H5a) tested the relationship between users' security attitudes and users' security behaviors. This hypothesis was accepted and confirmed the previous theoretical frameworks of TBP and DTPB and studies performed by Park and Chen (2007), Ng and Rahim (2005), and Ajzen (1988, 1991). The second hypothesis (H5b), the relationship between users' security intentions and users' security behaviors, was accepted and confirmed the finding of the previous studies.

Surprisingly, the third hypothesis (H5c), the relationship between users' perceived behavioral control and users' security behavior, was accepted only among employed respondents, represented by 70% of the sample. The finding of this hypothesis partially confirm the theory of the Decomposed Theory of Planned Behavior and study reported by Ng and Rahim (2005).

The hypothesis H5d showed that computing experience had a direct and positive affect on the adaptation of information security behavior. Mediator analyses revealed that computing experience had a significant effect only on the employed respondents. Finally, the hypothesis H5e was supported, indicating that previous breach experience could positively influence the adoption of information security technologies among smartphone users.

### **Research Implications**

Most of the previous studies have tried to improve security of information systems from software, firmware, and hardware perspective. However, this study has focused on the users of the smartphone. Smartphones are becoming one of the most convenient devices that



provide users with plenty of functionalities. These devices connect users to the Internet and enable them to browse; connect to social networks; send and receive emails; shop online; play games; store data; navigate with GPS and many other functions. Not only have these devices been used for personal uses, but they also have a myriad of business applications. The analyses of the demographics demonstrate that 94.8 % of the respondents to this research survey owned a smartphone and the mean number of years that respondents had used their smartphone was 3.4 years. This highlights the significance and popularity of smartphones among EMU's general student population. Because of these functions and this popularity, users store considerable sensitive information on their devices that require protection. Providing security in smartphone networks is vital and required for overall information security of individuals and businesses. Some of the methods that could provide the information security for smartphones include utilizing security technologies such as antivirus, antispysware, strong password development, occasional data back up, and encryption. Although most smartphones are equipped with these security technologies, several studies have shown that users often do not utilize them. To identify the factors that most affect users' behavior toward the adoption of these technologies, this study was designed and implemented. The study discovered those users' security attitudes, intentions, and subjective norms could have positive effects on users' behavior toward the adaptation of security technologies on their smartphones.

One of the main implications of this study would involve information security specialists, network security administrators, and information security educators. By focusing on the identified factors that have significant effects on users' attitudes, intentions, subjective norms, and perceived behavioral controls, the information security specialists and

information security educators could design and implement more robust and effective security plans and policies.

For instance, to change users' attitude toward using security technology, educational programs could be created that change users' perceptions regarding the usefulness of these technologies. Also, users could be taught about issues and outcomes regarding the severe consequences of security breach on their devices. From the analysis of the moderator variables, programs that are more specialized could be created for different male, female, employed, and unemployed persons to improve their attitudes toward these technologies.

Since the users' security intentions have a direct relationship to their actual use of security technologies, the information security specialist could generate awareness programs that target the influential people in a users' life such as peers, friends, managers, and professors, to name a few. The awareness programs could be spread through influential media such as the Internet, newspapers, and TV. Since perceived behavioral control has a significant relationship with security intention only in the female group, the educators and information security specialists could design customized programs and resources that could improve female group's self-efficacy and facilitating conditions, while programs customized to males' perceived behavioral control to foster greater security intention could also be offered.

In summary, this study has found that the theories of Planned Behavior, Technological Acceptance Model, Fear Appeals, and the Decomposed Theory of Planned Behavior apply in the field of information security, specifically in smartphone networks. The designers of information security programs and information security specialists could create plans that are more robust, demonstrate the ease with which security behaviors can be

applied, and show the importance of policies which could better protect their privacy and safety from risks. Such programs could affect users' behavior toward the utilization of security technologies. Individual and public networks would be more secure and smartphone users could reduce information security breaches, which have been proven to be costly and destructive. Moreover, this study introduced a research model based on the previous behavioral theories that could be applied in the field of information security.

### **Research Limitations and Future Studies**

This study has several limitations as described:

1. Due to the complexity of human behavior, this study could not identify all the variables that impact users' security behavior. There could be other latent variables that could be considered as predictors of the users' attitude, intention, subjective norm, and perceived behavioral control.
2. Due to the sampling process, most of the respondents were students enrolled at Eastern Michigan University. Selecting a more diverse sample could provide better insight regarding users' security behavior in smartphone networks. A more diverse sample may provide new insights into other moderator variables that could influence the key factors.
3. This study collected its sample size utilizing convenient and snowball sampling methods from the University's online daily announcements, Facebook page, and individual classes. This might affect the validity of the study. Hence, it is advisable to use different sampling procedures for more diverse sample size.
4. This research only examined the information security behavior from two perspectives: first, utilization of antivirus, antispyware, password, and backup

systems; and second, regularly updating antivirus, antispyware, passwords, and back up. Focusing on other types of security behavior such as using encryption, trusted websites, and/ or secure banking could enhance this study.

5. This study collected no information about the users' ethnicity or their languages. Since smartphone are used worldwide it would be beneficial and interesting to find out how ethnicity and language moderate the factors that impact users' security behaviors.
6. The ordering of the questions might create a mindset for the respondents that expect the same questions throughout the survey.
7. All of the questions have worded positively and there are no negative questions.

Based on the results of the research and the study limitations, the following future research is recommended:

1. The research model could be tested in more diverse sample size with more diverse ages.
2. The experimental studies could examine the developed research model.
3. Utilizing the developed research model, future studies could examine the impact of other factors on the users' security behavior.
4. Future studies could focus on the different security behaviors such as using encryptions, secure Internet browsing, and other available security technologies.
5. Since this study provides strong support for the application of socio-behavioral theories in information security in the smartphone networks, future studies could develop policies and educational programs to target the influential factors on users'

security behavior. The developed programs could be used in the control group for experimental studies.

6. Finally, future studies could focus and identify other variables that influence information security behavior in smartphone networks.
7. Future researches could create a survey that presents the questions randomly to reduce bias in the anticipation of the questions.
8. Future studies could reword and rearrange negative questions alongside positive ones.

## References

- Ajzen, I. (1988). *Attitudes, personality, and behavior*. Homewood, IL, US: Dorsey Press.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179–211.
- Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social. *Behaviour*. Englewood Cliffs, NJ: Prentice-Hall.
- Akarapanich, S. (2006). *Comparing customer loyalty intentions using trust, satisfaction, and commitment of online MBA students versus traditional MBA students*. Dissertation.
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34, 613–643.
- Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 103, 411.
- Androulidakis, I., & Kandus, G. (2011a). Mobile phone brand categorization vs. users' security practices. *Engineering, Technology & Applied Science Research*, 1(2), pp–30. Retrieved from <http://etasr.com/index.php/ETASR/article/view/19>
- Androulidakis, I., & Kandus, G. (2011b). Mobile phone security awareness and practices of students in budapest. In *ICDT 2011, The Sixth International Conference on Digital Telecommunications* (pp. 18–24). Retrieved from [http://www.thinkmind.org/index.php?view=article&articleid=icdt\\_2011\\_1\\_40\\_20110](http://www.thinkmind.org/index.php?view=article&articleid=icdt_2011_1_40_20110)
- Arbaugh, W. A. (2003). Wireless security is different. *Computer*, 36, 99–101.

- Bagozzi, R. P., & Heatherton, T. F. (1994). A general approach to representing multifaceted personality constructs: Application to state self-esteem. *Structural Equation Modeling: A Multidisciplinary Journal*, 1(1), 35–67.
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory* (Vol. xiii). Englewood Cliffs, NJ, US: Prentice-Hall, Inc.
- Benenson, Z., Kroll-Peters, O., & Krupp, M. (2012). Attitudes to IT security when using a smartphone. In *Computer Science and Information Systems (FedCSIS), 2012 Federated Conference on* (pp. 1179–1183). IEEE.
- Boone, H. N., & Boone, D. A. (2012). Analyzing likert data. *Journal of Extension*, 50(2), 1–5. Retrieved from <http://www.joe.org/joe/2012april/tt2.php>
- Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly*, 22, vii–xvi.
- Clarke, M. (2011). *The role of self-efficacy in computer security behavior: Developing the construct of computer security self-efficacy*. ProQuest LLC.
- Costello, A. B., & Osborne, J. W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment Research & Evaluation*, 10, 1–9.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35, 982–1003.

- Dehghan, A. (2012). *Student loyalty assessment with online master's programs*. Doctoral dissertation, Eastern Michigan University.
- DeVellis, R. F. (2011). *Scale Development: Theory and Applications* (Third Edition edition.). Thousand Oaks, Calif: SAGE Publications, Inc.
- Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73–80.
- Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes* (Vol. xxii). Orlando, FL, US: Harcourt Brace Jovanovich College Publishers.
- Egan, G., Haley, K., Mckinney, D., Millington, T., Mulcahy, J., Parsons, T., ... Hittel, S. (2012). *Internet security threat report*. Technical Report. April.
- Esmaeili, M., & Eydgahi, A. (2013). An evaluation model for project based active learning in an engineering technology freshman course. Presented at the International Conference on Engineering Education Research.
- Ferguson, M. J., & Bargh, J. A. (2007). Beyond the attitude object: Implicit attitudes spring from object-centered contexts. In B. Wittenbrink & N. Schwarz (Eds.), *Implicit measures of attitudes* (pp. 216–246). New York, NY, US: Guilford Press.
- Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research*, 440–452. Retrieved from <http://www.jstor.org/stable/3151718>
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39–50. Retrieved from <http://www.jstor.org/stable/3151312>



- Fossi, M., Turner, D., Johnson, E., Mack, T., Adams, T., Blackbird, J., ... others. (2009). *Symantec global internet security threat report*.
- Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, 26, 410–417.
- Galletta, D. F., & Polak, P. (2003). An empirical investigation of antecedents of Internet abuse in the workplace. *SIGHCI 2003 Proceedings*, 14.
- Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, 4(1), 7.
- Grace, D., Weaven, S., Bodey, K., Ross, M., & Weaven, K. (2012). Putting student evaluations into perspective: the course experience quality and satisfaction model (CEQS). *Studies in Educational Evaluation*, 38(2), 35–43.
- Grothmann, T., & Reusswig, F. (2006). People at risk of flooding: Why some residents take precautionary action while others do not. *Natural Hazards*, 38, 101–120.
- Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, 40, 414–433.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18, 106–125.
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34, 549–566.

- Jones, C. M., McCarthy, R. V., Halawi, L., & Mujtaba, B. (2010). Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. *Journal of International Technology and Information Management*, *19*, 43–56.
- Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*, 139–154. doi:10.1016/0268-4012(02)00105-6
- Kim, S. H. (2008). Moderating effects of job relevance and experience on mobile wireless technology acceptance: Adoption of a smartphone by individuals. *Information & Management*, *45*, 387–393.
- Kline, R. B. (2011). *Principles and practice of structural equation modeling*. Guilford press.
- Koufteros, X. (1999). Testing a model of pull production: A paradigm for manufacturing research using structural equation modeling. *Journal of Operations Management*, *17*, 467–488.
- Koufteros, X., Vonderembse, M., & Doll, W. (2001). Concurrent engineering and its consequences. *Journal of Operations Management*, *19*, 97–115.
- Kutluca, T. (2011). A study on computer usage and attitudes toward computers of prospective preschool teacher. *International Journal on New Trends in Education and Their Implications*, *2*(1), 1–17.
- Lamour, J. (2008). *Impact of user awareness and training of InfoSec practitioners on data security*. Doctoral dissertation, Walden University.
- Lazou, A., & Weir, G. R. (2011). Perceived risk and sensitive data on mobile devices. *Cyberforensics: Issue and Perspectives*, 183–196.

- Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, 27, 445–454.
- Mahabi, V. (2010). *Information security awareness: System administrators and end-users perspectives at florida state university*. Doctoral dissertation, The Florida State University.
- Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46, 815–825.
- Ng, B.-Y., & Rahim, M. (2005). A socio-behavioral study of home computer users' intention to practice security. In *In Proceedings of the Ninth Pacific Asia Conference on Information Systems* (pp. 7–10). Retrieved from <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1132&context=pacis2005>
- Ormrod, J. E., & Leedy, P. D. (2005). *Practical research: Planning and design*. New Jersey, Pearson Merrill Prentice hall.
- Park, Y., & Chen, J. V. (2007). Acceptance and adoption of the innovative use of smartphone. *Industrial Management & Data Systems*, 107, 1349–1365.
- Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, 115–143.
- Pyszczynski, T., Greenberg, J., & Solomon, S. (1997). Why do we need what we need? A terror management perspective on the roots of human social motivation. *Psychological Inquiry*, 8(1), 1–20.
- Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28, 816–826.

- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*, 93–114.
- Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology, 153–176*.
- Segars, A. H. (1997). Assessing the unidimensionality of measurement: A paradigm and illustration within the context of information systems research. *Omega, 25*, 107–121.
- Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31–41.
- Sprinthall, R. C., & Fisk, S. T. (1990). *Basic statistical analysis*. Prentice Hall Englewood Cliffs, NJ.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 147–169*.
- Summers, R. C. (1997). *Secure computing: Threats and safeguards* (Vol. 5). McGraw-Hill New York.
- Taylor, S., & Todd, P. (1995a). An integrated model of waste management behavior: A test of household recycling and composting intentions. *Environment and Behavior, 27*, 603–630.
- Taylor, S., & Todd, P. (1995b). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. *International Journal of Research in Marketing, 12*, 137–155.
- Taylor, S., & Todd, P. A. (1995c). Understanding information technology usage: A test of competing models. *Information Systems Research, 6*, 144–176.

- Todorova, D. (2013). *Exploring Lean Implementation Success Factors in Job Shop, Batch Shop, and Assembly Line Manufacturing Settings*. Doctoral dissertation, Eastern Michigan University.
- Weaver, J. B. (2011). *Hypothesis testing using z-and t-tests*. Blacksburg, VA: Virginia Polytechnic Institute and State University.
- Whitman, M., & Mattord, H. (2011). *Principles of information security*. Cengage Learning.
- Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 27*, 591–615.
- Wong, K. K.-K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin, 24*, 1–32.
- Woon, I., Tan, G.-W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In *ICIS 2005 Proceedings* (Vol. 26, p. 31).
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*, 2799–2816.
- Yushau, B. (2006). The effects of blended e-learning on mathematics and computer attitudes in pre-calculus algebra. *The Montana Mathematics Enthusiast, 3*, 176–183.

## Appendix

## **Appendix A**

### **Student Informed Consent Agreement**

#### **Purpose and Duration of This Research:**

This research is attempting to identify the factors that impact smartphone users' behavior toward the adaptation of security technologies such as antivirus, antispyware, and using password. The research will be conducted at Eastern Michigan University in Fall 2013 and Winter 2014 for a duration of two semesters.

#### **Subject Participation and Duration:**

This is a one-time survey being conducted for two school semesters of Fall semester 2013 and Winter 2014. It will take between 10 to 15 minutes to complete the survey. Your participation is completely voluntary and there are no rights or wrong answers to the survey questions. Also, there are no anticipated risks in taking this survey. If, at any time, you wish to discontinue your participation in the study, you may do so at any time.

#### **Benefits of this Research:**

The outcomes of this study will help information security specialists and organizations create safe information security systems. Also, the factors that impact users' intention to adopt security technologies and behaviors on smartphones can be beneficial toward the overall security of individual and public networks that most of us participate in.

#### **Dissemination of Research Results:**

The results of this study will be presented within the University (as PhD dissertation) and at regional and national conferences. This work will also be submitted for publication in academic journals.

The study is conducted through LimSurvey and your responses are anonymous. At no time will your name be associated with your responses to the questionnaires. Moreover, a LimeSurvey that has been hosted on one of the school's computer will not capture the IP addresses for further confidentiality. All data will be reported as aggregated results, which will be stored in a password protected secured computer.

### **Student consent**

I have read or have had read to me all of the above information about this research study, including the research procedures, duration of the study, and the likelihood of any benefit to me. The content and meaning of this information has been explained and I understand. All of my questions, at this time, have been answered. I hereby consent and do voluntarily offer to follow the study requirements and take part in the study by checking the button electronically showing my consent.

If you have any questions or concerns regarding this consent form, please contact:

Researcher:

Mohammadjafar Esmaili

PhD Student at College of Technology, Eastern Michigan University

[mesmaeil@emich.edu](mailto:mesmaeil@emich.edu)

734-219-2436

Advisor:

Dr. Ali Eydgahi

Professor at College of Technology, Eastern Michigan University

[aeydgahi@emich.edu](mailto:aeydgahi@emich.edu)

734-487-2049

***This research protocol and informed consent document has been reviewed and approved by the Eastern Michigan University Human Subjects Review Committee for use for Fall 2013 and Winter 2014. If you have any questions about the approval process, please contact Director of Graduate School. ( 734.487.0042, [human.subjects@emich.edu](mailto:human.subjects@emich.edu)).***



## Appendix B Human Subject Approval

**E**ASTERN MICHIGAN UNIVERSITY *Education First*

---

November 14, 2013

UHSRC INITIAL APPROVAL: EXEMPT

**To:** Mohammadjafar Esmaeili  
Eastern Michigan University

**Re:** UHSRC # 131015  
Category: Conditionally Exempt  
Approval Date: November 14, 2013

**Title:** Assessment of Users' Information Security Behavior in Smartphone Networks

The Eastern Michigan University Human Subjects Review Committee (UHSRC) has completed their review of your project. I am pleased to advise you that **your research has been deemed as exempt** in accordance with federal regulations.

The UHSRC has found that your research project meets the criteria for exempt status and the criteria for the protection of human subjects in exempt research. **Under our exempt policy the Principal Investigator assumes the responsibility for the protection of human subjects** in this project as outlined in the assurance letter and exempt educational material.

**Renewals:** Exempt protocols do not need to be renewed. If the project is completed, please submit the **Human Subjects Study Completion Form** (found on the UHSRC website).

**Revisions:** Exempt protocols do not require revisions. However, if changes are made to a protocol that may no longer meet the exempt criteria, a **Human Subjects Minor Modification Form** or new **Human Subjects Approval Request Form** (if major changes) will be required (see UHSRC website for forms).

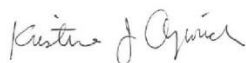
**Problems:** If issues should arise during the conduct of the research, such as unanticipated problems, adverse events, or any problem that may increase the risk to human subjects and change the category of review, notify the UHSRC office within 24 hours. Any complaints from participants regarding the risk and benefits of the project must be reported to the UHSRC.

**Follow-up:** If your exempt project is not completed and closed after three years, the UHSRC office will contact you regarding the status of the project and to verify that no changes have occurred that may affect exempt status.

Please use the UHSRC number listed above on any forms submitted that relate to this project, or on any correspondence with the UHSRC office.

Good luck in your research. If we can be of further assistance, please contact us at 734-487-0042 or via e-mail at [gs\\_human\\_subjects@emich.edu](mailto:gs_human_subjects@emich.edu). Thank you for your cooperation.

Sincerely,



Dr. Kristine Ajrouch  
Faculty Co-chair  
University Human Subjects Review Committee

---

University Human Subjects Review Committee · Eastern Michigan University · 200 Boone Hall  
Ypsilanti, Michigan 48197  
Phone: 734.487.0042 Fax: 734.487.0050  
E-mail: [human.subjects@emich.edu](mailto:human.subjects@emich.edu)  
[www.ord.emich.edu](http://www.ord.emich.edu) (see Federal Compliance)

The EMU UHSRC complies with the Title 45 Code of Federal Regulations part 46 (45 CFR 46) under FWA0000050.

## **Appendix C**

### **Descriptive analysis**

Each construct consists of several items and each item was assessed using a five-point Likert-type scale: Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4), and Strongly Agree (5). Since each construct has been generated from summation of several Likert-type items, this study treats each construct as an interval variable and provides descriptive statistics for each construct, i.e., mean, variance, standard deviation (Boone and Boone, 2012). Also, to analyze each item within a construct, item means, item variances, inter-item correlations, item-total statistics, etc. were calculated. After describing and providing details about each construct, this section reports the following sections for each scale and its items analysis from SPSS output:

- **Statistics for Scale:** Including Mean, Variance and Standard Deviation of the construct.
- **Item Statistics:** Including Mean, Variance and Standard Deviation for each item related to the construct.
- **Summary Item Statistics:** Including Means, Variances and Inter-Item Correlations for the set of items within a construct.
- **Item-total Statistics:** Including "Scale Mean if Item Deleted", "Scale Variance if Item Deleted", "Corrected Item-Total Correlation", "Squared Multiple Correlation" and "Cronbach's Alpha if Item Deleted".

#### **Security Behavior**

The Security Behavior scale was formed from summation of eight Likert-type items. Table 17 summarizes the Security Behavior construct for the eight individual items'

descriptive statistics; and the effect of the exclusion of each item on the overall reliability. The descriptive analysis and scale validity have been accessed from the “Analyze>>Scale>>Reliability Analysis” menu in SPSS. According to Table 17, the average mean of eight items is 2.878 with a variance of 1.984. The overall reliability of the Security Behavior is 0.779 and although eliminating the BEH8 (I am keeping sensitive personal data on my phone) will slightly increase the overall reliability, the research will continue without eliminating any items.

Table 17

*Security Behavior Item Analysis (N=593)*

| <b>Statistics for Scale</b>    | <b>Item</b>                       | <b>Mean</b>                           | <b>Variance</b>                         | <b>SD</b>                           | <b>Coefficient <math>\alpha</math></b>  |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
|                                | 8                                 | 23.02                                 | 49.910                                  | 7.065                               | 0.779                                   |
| <b>Item Statistics</b>         | <b>Mean</b>                       | <b>SD</b>                             | <b>N</b>                                |                                     |   |
| BEH1                           | 3.43                              | 1.688                                 | 593                                     |                                     |   |
| BEH2                           | 2.21                              | 1.263                                 | 593                                     |                                     |   |
| BEH3                           | 2.94                              | 1.489                                 | 593                                     |                                     |   |
| BEH4                           | 2.44                              | 1.438                                 | 593                                     |                                     |   |
| BEH5                           | 2.37                              | 1.391                                 | 593                                     |                                     |   |
| BEH6                           | 3.04                              | 1.410                                 | 593                                     |                                     |   |
| BEH7                           | 3.78                              | 1.189                                 | 593                                     |                                     |   |
| BEH8                           | 2.81                              | 1.344                                 | 593                                     |                                     |   |
| <b>Summary</b>                 | <b>Mean</b>                       | <b>Min.</b>                           | <b>Max.</b>                             | <b>Range</b>                        | <b>Max/Min</b>                          |
| <b>Means</b>                   | 2.878                             | 2.211                                 | 3.784                                   | 1.573                               | 1.712                                   |
| <b>Variiances</b>              | 1.984                             | 1.413                                 | 2.850                                   | 1.437                               | 2.017                                   |
| <b>Inter-Item Correlations</b> | .306                              | .079                                  | .907                                    | .828                                | 11.459                                  |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| BEH1                           | 19.60                             | 36.093                                | .541                                    | .545                                | .746                                    |

|      |       |        |      |      |      |
|------|-------|--------|------|------|------|
| BEH2 | 20.81 | 38.704 | .611 | .433 | .736 |
| BEH3 | 20.08 | 36.393 | .629 | .598 | .729 |
| BEH4 | 20.58 | 38.876 | .500 | .823 | .752 |
| BEH5 | 20.66 | 38.604 | .542 | .832 | .745 |
| BEH6 | 19.98 | 40.609 | .407 | .238 | .768 |
| BEH7 | 19.24 | 42.124 | .413 | .226 | .766 |
| BEH8 | 20.21 | 43.929 | .234 | .081 | .793 |

### Security Intention

Security intention was measured using six Likert-type items. Table 18 summarized the descriptive Security Intention analysis along with its items. The scale's reliability is 0.85 and excluding any of the items does not increase the value of the Cronbach's alpha coefficient. The average mean of items is 2.96 with a variance of 1.79. Except IN1 with a mean of 2.99, the rest of the items have a lower mean than the average mean.

Table 18

#### *Security Intention Descriptive Analysis (N=593)*

| Statistics for Scale    | Item  | Mean  | Variance | SD    | Coefficient $\alpha$ |
|-------------------------|-------|-------|----------|-------|----------------------|
|                         | 6     | 17.7  | 37.181   | 6.098 | 0.779                |
| Item Statistics         | Mean  | SD    |          |       |                      |
| IN1                     | 2.99  | 1.345 |          |       |                      |
| IN2                     | 2.63  | 1.296 |          |       |                      |
| IN3                     | 2.76  | 1.367 |          |       |                      |
| IN4                     | 2.73  | 1.358 |          |       |                      |
| IN5                     | 3.36  | 1.305 |          |       |                      |
| IN6                     | 3.29  | 1.361 |          |       |                      |
| Summary                 | Mean  | Min.  | Max.     | Range | Max/Min              |
| Means                   | 2.961 | 2.626 | 3.361    | .735  | 1.280                |
| Variances               | 1.793 | 1.681 | 1.870    | .189  | 1.113                |
| Inter-Item Correlations | .491  | .323  | .928     | .605  | 2.873                |

| <b>Item-Total Statistics</b> | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
|------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
| IN1                          | 14.77                             | 27.317                                | .573                                    | .441                                | .840                                    |
| IN2                          | 15.14                             | 26.758                                | .652                                    | .502                                | .826                                    |
| IN3                          | 15.01                             | 26.008                                | .667                                    | .864                                | .823                                    |
| IN4                          | 15.04                             | 25.882                                | .684                                    | .866                                | .819                                    |
| IN5                          | 14.41                             | 27.286                                | .601                                    | .816                                | .835                                    |
| IN6                          | 14.48                             | 26.233                                | .653                                    | .829                                | .826                                    |

### Security Attitude

Security attitudes were constructed of six Likert-type items. The descriptive analysis of security attitude has been presented in Table 19. The average mean of six items is 3.966 with a variance of 1.033. ATT2, ATT3, and ATT4 are under the average mean and the rest of the items are above the mean average. The scale reliability is 0.87; excluding any of the items will not increase the scale reliability.

Table 19

#### *Security Attitude Descriptive Analysis (N=593)*

| <b>Statistics for Scale</b> | <b>Item</b> | <b>Mean</b> | <b>Variance</b> | <b>SD</b>    | <b>Coefficient <math>\alpha</math></b> |
|-----------------------------|-------------|-------------|-----------------|--------------|--|
|                             | 6           | 23.80       | 22.314          | 4.724        | 0.867                                  |
| <b>Item Statistics</b>      | <b>Mean</b> | <b>SD</b>   |                 |              |  |
| ATT1                        | 4.13        | 1.032       |                 |              |  |
| ATT2                        | 3.83        | 1.052       |                 |              |  |
| ATT3                        | 3.75        | 1.102       |                 |              |  |
| ATT4                        | 3.79        | 1.073       |                 |              |  |
| ATT5                        | 4.17        | .900        |                 |              |  |
| ATT6                        | 4.13        | .923        |                 |              |  |
| <b>Summary</b>              | <b>Mean</b> | <b>Min.</b> | <b>Max.</b>     | <b>Range</b> | <b>Max/Min</b>                         |

|                                |                                   |                                       |   |                                     |   |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
| <b>Means</b>                   | 3.966                             | 3.749                                 | 4.169                                   | .420                                | 1.112                                   |
| <b>Variiances</b>              | 1.033                             | .809                                  | 1.215                                   | .406                                | 1.502                                   |
| <b>Inter-Item Correlations</b> | .523                              | .400                                  | .909                                    | .509                                | 2.271                                   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| ATT1                           | 19.66                             | 16.176                                | .611                                    | .501                                | .853                                    |
| ATT2                           | 19.97                             | 15.644                                | .668                                    | .544                                | .843                                    |
| ATT3                           | 20.05                             | 15.195                                | .687                                    | .829                                | .840                                    |
| ATT4                           | 20.01                             | 15.189                                | .714                                    | .835                                | .835                                    |
| ATT5                           | 19.63                             | 16.646                                | .662                                    | .788                                | .845                                    |
| ATT6                           | 19.67                             | 16.603                                | .646                                    | .783                                | .847                                    |

### Subjective Norm (SN)

The construct of Subjective Norm consisted of six Likert-type items. With a value of Cronbach's Alpha coefficient of 0.91, deleting any of the individual items would not improve the overall Cronbach's Alpha coefficient. The average mean of the SN is 3.506 with a variance of 1.235. From the constructing items only SN1, SN3, SN4 are below the average mean.

Table 20

### Subjective Norm Descriptive Analysis (N=593)

| <b>Statistics for Scale</b> | <b>Item</b> | <b>Mean</b> | <b>Variance</b> | <b>SD</b> | <b>Coefficient <math>\alpha</math></b> |
|-----------------------------|-------------|-------------|-----------------|-----------|--|
|                             | 6           | 21.04       | 30.514          | 5.524     | 0.91                                   |
| <b>Item Statistics</b>      | <b>Mean</b> | <b>SD</b>   |                 |           |  |
| SN1                         | 3.41        | 1.134       |                 |           |  |
| SN2                         | 3.67        | 1.121       |                 |           |  |
| SN3                         | 3.26        | 1.146       |                 |           |  |
| SN4                         | 3.39        | 1.136       |                 |           |  |
| SN5                         | 3.64        | 1.052       |                 |           |  |

| SN6                            | 3.66                              | 1.076                                 |   |                                     |   |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
| <b>Summary</b>                 | Mean                              | Min.                                  | Max.                                    | Range                               |   |
| <b>Means</b>                   | 3.506                             | 3.256                                 | 3.675                                   | .418                                |   |
| <b>Variances</b>               | 1.235                             | 1.107                                 | 1.313                                   | .206                                |   |
| <b>Inter-Item Correlations</b> | .624                              | .518                                  | .809                                    | .292                                |   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| SN1                            | 17.62                             | 21.695                                | .713                                    | .589                                | .897                                    |
| SN2                            | 17.36                             | 21.386                                | .759                                    | .642                                | .890                                    |
| SN3                            | 17.78                             | 21.348                                | .742                                    | .731                                | .893                                    |
| SN4                            | 17.64                             | 21.115                                | .777                                    | .760                                | .888                                    |
| SN5                            | 17.40                             | 22.098                                | .739                                    | .724                                | .893                                    |
| SN6                            | 17.37                             | 21.822                                | .750                                    | .752                                | .892                                    |

### Perceived Behavioral Control (PBC)

The construct of PBC consists of the sum of six Likert-type items. Table 21 demonstrates the item-analysis results along with the average mean and the impact of each item on the overall reliability of the PBC. The average mean of the six items is 4.157 with a variance of 1.081. Exclusion of any item would not increase the value of Cronbach's Alpha. Therefore all six items were retained. As presented in the following table only PBC3, PBC4, and PBC6 are slightly below average and the rest are above average.

Table 21

#### *Perceived Behavioral Control Descriptive Analysis (N=593)*

| <b>Statistics for Scale</b> | <b>Item</b> | <b>Mean</b> | <b>Variance</b> | <b>SD</b> | <b>Coefficient <math>\alpha</math></b> |
|-----------------------------|-------------|-------------|-----------------|-----------|--|
|                             | 6           | 24.94       | 23.902          | 4.889     | 0.874                                  |
| <b>Item Statistics</b>      |             | <b>Mean</b> |                 | <b>SD</b> |  |
| PBC1                        |             | 4.44        |                 | .866      |  |

|                                |                                   |                                       |   |                                     |   |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
| PBC2                           | 4.42                              |                                       | .882                                    |                                     |   |
| PBC3                           | 3.95                              |                                       | 1.163                                   |                                     |   |
| PBC4                           | 3.67                              |                                       | 1.307                                   |                                     |   |
| PBC5                           | 4.33                              |                                       | .883                                    |                                     |   |
| PBC6                           | 4.14                              |                                       | 1.057                                   |                                     |   |
| <b>Summary</b>                 | Mean                              | Min.                                  | Max.                                    | Range                               | Max/Min                                 |
| <b>Means</b>                   | 4.157                             | 3.668                                 | 4.440                                   | .772                                | 1.211                                   |
| <b>Variances</b>               | 1.081                             | .750                                  | 1.709                                   | .958                                | 2.278                                   |
| <b>Inter-Item Correlations</b> | .561                              | .323                                  | .782                                    | .458                                | 2.418                                   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| PBC1                           | 20.50                             | 18.294                                | .656                                    | .666                                | .858                                    |
| PBC2                           | 20.52                             | 17.824                                | .712                                    | .679                                | .850                                    |
| PBC3                           | 20.99                             | 16.095                                | .692                                    | .714                                | .851                                    |
| PBC4                           | 21.27                             | 15.664                                | .631                                    | .711                                | .869                                    |
| PBC5                           | 20.61                             | 17.590                                | .747                                    | .720                                | .845                                    |
| PBC6                           | 20.80                             | 16.625                                | .714                                    | .711                                | .846                                    |

### Perceived Usefulness (PU)

The construct of Perceived Usefulness consists of the sum of five items. The items analysis is presented in Table 22 along with the PU scale descriptive analysis. As demonstrated in Table 22, eliminating any items would not increase the scale's alpha value of .88; all items were retained for future analysis. The average mean is 4.015 with a variance of 0.957. Items PU2 and PU3 have a lower mean when compared with the average mean. Also, the PU has a reliability of 0.875, which is above the acceptable range of 0.7.

Table 22

#### *Perceived Usefulness Descriptive Analysis (N=593)*

| <b>Statistics</b> | <b>Item</b> | <b>Mean</b> | <b>Variance</b> | <b>SD</b> | <b>Coefficient <math>\alpha</math></b> |
|-------------------|-------------|-------------|-----------------|-----------|--|
|-------------------|-------------|-------------|-----------------|-----------|--|



| <b>for Scale</b>               | 5                                 | 20.07                                 | 15.947                                  | 3.993                               | 0.875                                   |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
| <b>Item Statistics</b>         | <b>Mean</b>                       |                                       | <b>SD</b>                               |                                     |   |
| PU1                            | 4.11                              |                                       | .966                                    |                                     |   |
| PU2                            | 3.94                              |                                       | 1.028                                   |                                     |   |
| PU3                            | 3.75                              |                                       | 1.061                                   |                                     |   |
| PU4                            | 4.16                              |                                       | .898                                    |                                     |   |
| PU5                            | 4.12                              |                                       | .929                                    |                                     |   |
| <b>Summary</b>                 | <b>Mean</b>                       | <b>Min.</b>                           | <b>Max.</b>                             | <b>Range</b>                        | <b>Max/Min</b>                          |
| <b>Means</b>                   | 4.015                             | 3.747                                 | 4.164                                   | .417                                | 1.111                                   |
| <b>Variances</b>               | .957                              | .806                                  | 1.125                                   | .319                                | 1.396                                   |
| <b>Inter-Item Correlations</b> | .590                              | .458                                  | .824                                    | .365                                | 1.797                                   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| PU1                            | 15.96                             | 10.336                                | .753                                    | .673                                | .837                                    |
| PU2                            | 16.14                             | 10.113                                | .731                                    | .672                                | .842                                    |
| PU3                            | 16.33                             | 10.717                                | .591                                    | .374                                | .878                                    |
| PU4                            | 15.91                             | 10.801                                | .735                                    | .721                                | .842                                    |
| PU5                            | 15.96                             | 10.659                                | .730                                    | .713                                | .843                                    |

### Perceived Ease of Use (PEU)

The construct of PEU consists of five Likert-type items. Analyses of the construct of PEU and its items are presented in Table 23. The average mean of the items is 3.838 with a variance of 1.253. The reliability of the PEU is 0.83, which is in the acceptable range. Items PEU3 and PEU4 have a lower mean than the average mean.

Table 23

#### *Perceived Ease of Use Descriptive Analysis (N=593)*

| <b>Statistics for Scale</b> | <b>Item</b> | <b>Mean</b> | <b>Variance</b> | <b>SD</b> | <b>Coefficient <math>\alpha</math></b> |
|-----------------------------|-------------|-------------|-----------------|-----------|--|
|                             | 5           | 19.19       | 18.740          | 4.329     | 0.832                                  |

| <b>Item Statistics</b>         | <b>Mean</b>                       |                                       | <b>SD</b>                               |                                     |   |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
| PEU1                           |                                   | 4.35                                  |   | .943                                |   |
| PEU2                           |                                   | 4.25                                  |   | .992                                |   |
| PEU3                           |                                   | 3.33                                  |   | 1.251                               |   |
| PEU4                           |                                   | 3.37                                  |   | 1.258                               |   |
| PEU5                           |                                   | 3.89                                  |   | 1.115                               |   |
| <b>Summary</b>                 | <b>Mean</b>                       | <b>Min.</b>                           | <b>Max.</b>                             | <b>Range</b>                        | <b>Max/Min</b>                          |
| <b>Means</b>                   | 3.838                             | 3.334                                 | 4.349                                   | 1.015                               | 1.305                                   |
| <b>Variances</b>               | 1.253                             | .890                                  | 1.583                                   | .693                                | 1.779                                   |
| <b>Inter-Item Correlations</b> | .504                              | .302                                  | .937                                    | .635                                | 3.104                                   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| PEU1                           | 14.84                             | 13.751                                | .586                                    | .762                                | .812                                    |
| PEU2                           | 14.94                             | 13.191                                | .633                                    | .776                                | .800                                    |
| PEU3                           | 15.86                             | 11.392                                | .685                                    | .880                                | .783                                    |
| PEU4                           | 15.82                             | 11.342                                | .686                                    | .880                                | .783                                    |
| PEU5                           | 15.31                             | 12.807                                | .588                                    | .362                                | .811                                    |

### Perceived Probability (PP)

The construct of Perceived Probability has been formed by the summation of six items. The construct and items analysis has been presented in Table 24. The average mean is 2.889 with a variance of 1.481. Items PP2, PP3, and PP4 have a lower mean than the overall mean, but the rest of the items are above the average mean. Also, the estimated Cronbach's Alpha coefficient reliability is 0.896 with is acceptable and above 0.7.

Table 24

#### *Perceived Probability Descriptive Analysis (N=593)*

| <b>Statistics for Scale</b> | <b>Item</b> | <b>Mean</b> | <b>Variance</b> | <b>SD</b> | <b>Coefficient <math>\alpha</math></b> |
|-----------------------------|-------------|-------------|-----------------|-----------|--|
|                             | 6           | 17.34       | 35.038          | 5.919     | 0.896                                  |

| <b>Item Statistics</b>         | <b>Mean</b>                       |                                       | <b>SD</b>                               |                                     |   |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
| PP1                            | 3.13                              |                                       | 1.251                                   |                                     |   |
| PP2                            | 2.86                              |                                       | 1.241                                   |                                     |   |
| PP3                            | 2.46                              |                                       | 1.105                                   |                                     |   |
| PP4                            | 2.60                              |                                       | 1.182                                   |                                     |   |
| PP5                            | 3.28                              |                                       | 1.253                                   |                                     |   |
| PP6                            | 3.01                              |                                       | 1.263                                   |                                     |   |
| <b>Summary</b>                 | Mean                              | Min.                                  | Max.                                    | Range                               | Max/Min                                 |
| <b>Means</b>                   | 2.889                             | 2.462                                 | 3.280                                   | .818                                | 1.332                                   |
| <b>Variances</b>               | 1.481                             | 1.222                                 | 1.596                                   | .374                                | 1.306                                   |
| <b>Inter-Item Correlations</b> | .590                              | .458                                  | .844                                    | .385                                | 1.841                                   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| PP1                            | 14.20                             | 24.869                                | .690                                    | .660                                | .882                                    |
| PP2                            | 14.48                             | 24.375                                | .745                                    | .695                                | .873                                    |
| PP3                            | 14.87                             | 26.026                                | .691                                    | .715                                | .882                                    |
| PP4                            | 14.74                             | 24.869                                | .744                                    | .752                                | .873                                    |
| PP5                            | 14.06                             | 24.620                                | .711                                    | .669                                | .878                                    |
| PP6                            | 14.33                             | 24.279                                | .736                                    | .682                                | .875                                    |

### Perceived Severity (PS)

The construct of Perceived Severity, which measures the respondent's perceived severity of a security breach, consists of six Likert-type items. The construct and the items descriptive analysis is presented in Table 25. The average mean is 3.20 with a variance of 1.53.

As demonstrated in Table 25 the average mean is 3.197 with a variance of 1.527. The only items that have a lower mean than average mean are PS1 and PS2.

Table 25

*Perceived Severity Descriptive Analysis (N=593)*

| <b>Statistics for Scale</b>    | <b>Item</b>                       | <b>Mean</b>                           | <b>Variance</b>                         | <b>SD</b>                           | <b>Coefficient <math>\alpha</math></b>  |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
|                                | 6                                 | 19.18                                 | 41.190                                  | 6.418                               | 0.993                                   |
| <b>Item Statistics</b>         | <b>Mean</b>                       | <b>SD</b>                             |   |                                     |   |
| PS1                            | 2.98                              | 1.262                                 |   |                                     |   |
| PS2                            | 3.10                              | 1.257                                 |   |                                     |   |
| PS3                            | 3.34                              | 1.192                                 |   |                                     |   |
| PS4                            | 3.34                              | 1.194                                 |   |                                     |   |
| PS5                            | 3.22                              | 1.250                                 |   |                                     |   |
| PS6                            | 3.20                              | 1.257                                 |   |                                     |   |
| <b>Summary Means</b>           | <b>Mean</b>                       | <b>Min.</b>                           | <b>Max.</b>                             | <b>Range</b>                        | <b>Max/Min</b>                          |
| <b>Means</b>                   | 3.197                             | 2.985                                 | 3.344                                   | .359                                | 1.120                                   |
| <b>Variiances</b>              | 1.527                             | 1.422                                 | 1.593                                   | .171                                | 1.120                                   |
| <b>Inter-Item Correlations</b> | .699                              | .599                                  | .869                                    | .270                                | 1.452                                   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| PS1                            | 16.20                             | 28.659                                | .810                                    | .760                                | .920                                    |
| PS2                            | 16.08                             | 28.725                                | .808                                    | .765                                | .920                                    |
| PS3                            | 15.84                             | 29.845                                | .762                                    | .794                                | .926                                    |
| PS4                            | 15.85                             | 29.448                                | .796                                    | .814                                | .922                                    |
| PS5                            | 15.96                             | 28.749                                | .811                                    | .795                                | .920                                    |
| PS6                            | 15.99                             | 28.496                                | .828                                    | .808                                | .917                                    |

**People Influence (PI)**

The construct of PI, which measures the external influence of other people on smartphone users' information security technology adaptation, consists of nine Likert-type items. The construct and items descriptive analysis is shown in Table 26. The estimated Cronbach's Alpha coefficient reliability is a near perfect 0.99. The average mean is 3.31

with a variance of 1.37. Items PI1, PI3, PI7, PI8, and PI9 have higher mean than the overall average mean.

Table 26

*People's Influence Descriptive Analysis (N=593)*

| <b>Statistics for Scale</b>    | <b>Item</b>                       | <b>Mean</b>                           | <b>Variance</b>                         | <b>SD</b>                           | <b>Coefficient <math>\alpha</math></b>  |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
|                                | 9                                 | 29.80                                 | 74.595                                  | 8.637                               | 0.99                                    |
| <b>Item Statistics</b>         | <b>Mean</b>                       | <b>SD</b>                             |   |                                     |   |
| PI1                            | 3.43                              | 1.166                                 |   |                                     |   |
| PI2                            | 3.26                              | 1.230                                 |   |                                     |   |
| PI3                            | 3.40                              | 1.193                                 |   |                                     |   |
| PI4                            | 3.09                              | 1.162                                 |   |                                     |   |
| PI5                            | 3.04                              | 1.198                                 |   |                                     |   |
| PI6                            | 3.21                              | 1.164                                 |   |                                     |   |
| PI7                            | 3.45                              | 1.119                                 |   |                                     |   |
| PI8                            | 3.39                              | 1.171                                 |   |                                     |   |
| PI9                            | 3.52                              | 1.137                                 |   |                                     |   |
| <b>Summary</b>                 | <b>Mean</b>                       | <b>Min.</b>                           | <b>Max.</b>                             | <b>Range</b>                        | <b>Max/Min</b>                          |
| <b>Means</b>                   | 3.311                             | 3.042                                 | 3.523                                   | .481                                | 1.158                                   |
| <b>Variances</b>               | 1.372                             | 1.251                                 | 1.512                                   | .260                                | 1.208                                   |
| <b>Inter-Item Correlations</b> | .630                              | .462                                  | .841                                    | .378                                | 1.819                                   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| PI1                            | 26.37                             | 59.434                                | .768                                    | .741                                | .932                                    |
| PI2                            | 26.54                             | 58.198                                | .793                                    | .788                                | .930                                    |
| PI3                            | 26.40                             | 58.730                                | .790                                    | .784                                | .930                                    |
| PI4                            | 26.71                             | 58.943                                | .802                                    | .812                                | .930                                    |
| PI5                            | 26.76                             | 58.622                                | .792                                    | .829                                | .930                                    |
| PI6                            | 26.59                             | 59.296                                | .778                                    | .796                                | .931                                    |
| PI7                            | 26.35                             | 60.377                                | .746                                    | .694                                | .933                                    |
| PI8                            | 26.41                             | 60.478                                | .700                                    | .764                                | .935                                    |
| PI9                            | 26.28                             | 60.441                                | .727                                    | .773                                | .934                                    |

### Media Influence (MI)

Media influence is another external factor designed to measure the impact of external forces such as the media on the adaptation of information security technology among users of smartphones. This variable consists of six Likert-type items. The variable of media influence and its constructed items descriptive analysis is presented in Table 27. The calculated average mean is 3.384 with a variance of 1.328. The calculated Cronbach's Alpha coefficient is 0.94. All of the items are retained since none of them increase the Alpha coefficient.

Table 27

#### *Descriptive Analysis of Media's Influence (N=593)*

| <b>Statistics for Scale</b>    | <b>Item</b>                       | <b>Mean</b>                           | <b>Variance</b>                         | <b>SD</b>                           | <b>Coefficient <math>\alpha</math></b>  |      |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|------|
|                                | 6                                 | 20.30                                 | 36.553                                  | 6.046                               | 0.94                                    |      |
| <b>Item Statistics</b>         |                                   | <b>Mean</b>                           |   | <b>SD</b>                           |   |      |
|                                | MI1                               | 3.52                                  |   | 1.164                               |   |      |
|                                | MI2                               | 3.37                                  |   | 1.163                               |   |      |
|                                | MI3                               | 3.30                                  |   | 1.166                               |   |      |
|                                | MI4                               | 3.16                                  |   | 1.159                               |   |      |
|                                | MI5                               | 3.56                                  |   | 1.115                               |   |      |
|                                | MI6                               | 3.39                                  |   | 1.147                               |   |      |
| <b>Summary Means</b>           | Mean                              | Min.                                  | Max.                                    | Range                               | Max/Min                                 |      |
|                                | 3.384                             | 3.159                                 | 3.558                                   | .400                                | 1.127                                   |      |
| <b>Variations</b>              | 1.328                             | 1.244                                 | 1.360                                   | .116                                | 1.093                                   |      |
| <b>Inter-Item Correlations</b> | .717                              | .624                                  | .870                                    | .246                                | 1.394                                   |      |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |      |
|                                | MI1                               | 16.78                                 | 25.764                                  | .798                                | .782                                    | .929 |
|                                | MI2                               | 16.93                                 | 25.373                                  | .839                                | .814                                    | .924 |
|                                | MI3                               | 17.00                                 | 25.731                                  | .800                                | .821                                    | .929 |
|                                | MI4                               | 17.15                                 | 25.577                                  | .822                                | .841                                    | .926 |

|     |       |        |      |      |      |
|-----|-------|--------|------|------|------|
| MI5 | 16.75 | 26.079 | .810 | .754 | .928 |
| MI6 | 16.91 | 25.658 | .824 | .792 | .926 |

### Self-Efficacy (SE)

As illustrated in Table 28, the construct of self-efficacy was created from summation of six Likert-scale items. The calculated reliability is 0.89, which is above 0.7 and significant. The average mean of the items is 3.913 with a variance of 1.246. The only items that have a lower mean than average are SE3 and SE4.

Table 28

#### *Descriptive Analysis of Self-Efficacy (N=593)*

| Statistics for Scale    | Item                       | Mean                           | Variance                         | SD                           | Coefficient $\alpha$             |
|-------------------------|----------------------------|--------------------------------|----------------------------------|------------------------------|----------------------------------|
|                         | 6                          | 23.48                          | 28.912                           | 5.377                        | 0.89                             |
| Item Statistics         | Mean                       | SD                             |                                  |                              |                                  |
| SE1                     | 4.14                       | 1.025                          |                                  |                              |                                  |
| SE2                     | 4.18                       | .991                           |                                  |                              |                                  |
| SE3                     | 3.52                       | 1.260                          |                                  |                              |                                  |
| SE4                     | 3.61                       | 1.246                          |                                  |                              |                                  |
| SE5                     | 3.98                       | 1.100                          |                                  |                              |                                  |
| SE6                     | 4.05                       | 1.047                          |                                  |                              |                                  |
| Summary                 | Mean                       | Min.                           | Max.                             | Range                        | Max/Min                          |
| Means                   | 3.913                      | 3.516                          | 4.184                            | .668                         | 1.190                            |
| Variances               | 1.246                      | .981                           | 1.588                            | .607                         | 1.618                            |
| Inter-Item Correlations | .581                       | .427                           | .885                             | .458                         | 2.074                            |
| Item-Total Statistics   | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Squared Multiple Correlation | Cronbach's Alpha if Item Deleted |
| SE1                     | 19.34                      | 21.498                         | .670                             | .742                         | .876                             |
| SE2                     | 19.30                      | 21.387                         | .714                             | .765                         | .870                             |
| SE3                     | 19.96                      | 19.674                         | .684                             | .832                         | .876                             |
| SE4                     | 19.87                      | 19.441                         | .721                             | .842                         | .869                             |
| SE5                     | 19.50                      | 20.365                         | .739                             | .803                         | .865                             |

|     |       |        |      |      |      |
|-----|-------|--------|------|------|------|
| SE6 | 19.43 | 20.759 | .740 | .811 | .866 |
|-----|-------|--------|------|------|------|

### Facilitating Condition (FC)

Facilitating conditions, which measure the impact of the availability of external resources on users' adaptations of information security technologies on smartphones, consists of three Likert-type items. As illustrated in Table 29, the average mean of items is 3.902 with a variance of 1.291.

Table 29

*Descriptive Analysis of Facilitating Condition (N=593)*

| Statistics for Scale           | Item                       | Mean                           | Variance                         | SD                           | Coefficient $\alpha$             |
|--------------------------------|----------------------------|--------------------------------|----------------------------------|------------------------------|----------------------------------|
|                                | 3                          | 11.70                          | 8.499                            | 2.915                        | 0.816                            |
| Item Statistics                | Mean                       | SD                             |                                  |                              |                                  |
| FC1                            | 4.21                       | 1.016                          |                                  |                              |                                  |
| FC2                            | 3.61                       | 1.254                          |                                  |                              |                                  |
| FC3                            | 3.88                       | 1.126                          |                                  |                              |                                  |
| Summary                        | Mean                       | Min.                           | Max.                             | Range                        | Max/Min                          |
| <b>Means</b>                   | 3.902                      | 3.614                          | 4.207                            | .594                         | 1.164                            |
| <b>Variances</b>               | 1.291                      | 1.033                          | 1.572                            | .539                         | 1.522                            |
| <b>Inter-Item Correlations</b> | .602                       | .540                           | .652                             | .112                         | 1.208                            |
| Item-Total Statistics          | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Squared Multiple Correlation | Cronbach's Alpha if Item Deleted |
| FC1                            | 7.50                       | 4.683                          | .633                             | .411                         | .787                             |
| FC2                            | 8.09                       | 3.708                          | .667                             | .457                         | .759                             |
| FC3                            | 7.82                       | 3.982                          | .723                             | .522                         | .692                             |

### Breach Experience (BE)



The construct of Breach Experience, which was designed to examine the respondents' own experience with information security breaches, has been constructed using five Likert-type items. Table 30 demonstrates the descriptive analysis of BE along with constructing items. The average mean of BE is 1.980 with a variance of 1.451. The calculated reliability is 0.858 which is within acceptable range.

Table 30

*Descriptive Analysis of Breach Experience (N=593)*

| <b>Statistics for Scale</b>    | <b>Item</b>                       | <b>Mean</b>                           | <b>Variance</b>                         | <b>SD</b>                           | <b>Coefficient <math>\alpha</math></b>  |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
|                                | 5                                 | 9.90                                  | 23.157                                  | 4.812                               | 0.858                                   |
| <b>Item Statistics</b>         | <b>Mean</b>                       | <b>SD</b>                             |   |                                     |   |
| BE1                            | 1.98                              | 1.154                                 |   |                                     |   |
| BE2                            | 2.18                              | 1.310                                 |   |                                     |   |
| BE3                            | 1.96                              | 1.184                                 |   |                                     |   |
| BE4                            | 1.97                              | 1.277                                 |   |                                     |   |
| BE5                            | 1.81                              | 1.083                                 |   |                                     |   |
| <b>Summary Means</b>           | Mean                              | Min.                                  | Max.                                    | Range                               | Max/Min                                 |
| <b>Variations</b>              | 1.980                             | 1.811                                 | 2.180                                   | .369                                | 1.204                                   |
| <b>Inter-Item Correlations</b> | 1.451                             | 1.174                                 | 1.716                                   | .542                                | 1.462                                   |
|                                | .553                              | .491                                  | .615                                    | .124                                | 1.252                                   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| BE1                            | 7.92                              | 15.730                                | .666                                    | .458                                | .831                                    |
| BE2                            | 7.72                              | 14.695                                | .672                                    | .464                                | .831                                    |
| BE3                            | 7.94                              | 15.753                                | .639                                    | .436                                | .838                                    |
| BE4                            | 7.93                              | 14.831                                | .681                                    | .483                                | .828                                    |
| BE5                            | 8.09                              | 15.717                                | .730                                    | .556                                | .817                                    |

**Computing Experience (CE)**

The construct of computing experience was constructed of five items, presented in Table 31. The average mean of the CE is 3.937 with a variance of 0.909. The Items CE4 and CE5 have a mean lower than the average. The calculated reliability is 0.864, which is acceptable.

Table 31

*Descriptive Analysis of Computing Experience (N=593)*

| <b>Statistics for Scale</b>    | <b>Item</b>                       | <b>Mean</b>                           | <b>Variance</b>                         | <b>SD</b>                           | <b>Coefficient <math>\alpha</math></b>  |
|--------------------------------|-----------------------------------|---------------------------------------|---|-------------------------------------|---|
|                                | 5                                 | 19.68                                 | 14.710                                  | 3.835                               | 0.864                                   |
| <b>Item Statistics</b>         | <b>Mean</b>                       | <b>SD</b>                             |   |                                     |   |
| CE1                            | 4.23                              | .800                                  |   |                                     |   |
| CE2                            | 4.33                              | .754                                  |   |                                     |   |
| CE3                            | 3.97                              | .970                                  |   |                                     |   |
| CE4                            | 3.60                              | 1.065                                 |   |                                     |   |
| CE5                            | 3.55                              | 1.123                                 |   |                                     |   |
| <b>Summary</b>                 | <b>Mean</b>                       | <b>Min.</b>                           | <b>Max.</b>                             | <b>Range</b>                        | <b>Max/Min</b>                          |
| <b>Means</b>                   | 3.937                             | 3.553                                 | 4.329                                   | .776                                | 1.218                                   |
| <b>Variances</b>               | .909                              | .569                                  | 1.261                                   | .692                                | 2.216                                   |
| <b>Inter-Item Correlations</b> | .578                              | .445                                  | .782                                    | .337                                | 1.758                                   |
| <b>Item-Total Statistics</b>   | <b>Scale Mean if Item Deleted</b> | <b>Scale Variance if Item Deleted</b> | <b>Corrected Item-Total Correlation</b> | <b>Squared Multiple Correlation</b> | <b>Cronbach's Alpha if Item Deleted</b> |
| CE1                            | 15.45                             | 10.383                                | .716                                    | .667                                | .832                                    |
| CE2                            | 15.35                             | 10.736                                | .689                                    | .657                                | .840                                    |
| CE3                            | 15.71                             | 9.726                                 | .669                                    | .534                                | .839                                    |
| CE4                            | 16.09                             | 9.077                                 | .702                                    | .642                                | .833                                    |
| CE5                            | 16.13                             | 8.752                                 | .707                                    | .655                                | .833                                    |