Informatics in Education, 2016, Vol. 15, No. 2, 235–252

DOI: 10.15388/infedu.2016.12

On Mobile Device Security Practices and Training Efficacy: An Empirical Study

Amita GOYAL CHIN[1], Ugochukwu ETUDO[1], Mark A. HARRIS[2]
[1]*Department of Information Systems, School of Business, Virginia Commonwealth University*
P.O. Box 844000, Richmond, Virginia 23284-4000
[2]*Augusta University Cyber Institute*
1120 15th Street, University Hall/UH-127, Augusta, Georgia 30912
e-mail: agchin@vcu.edu, etudouo@vcu.edu, marharris1@augusta.edu

Received: May 2016

Abstract. The past decade has witnessed an explosion of the penetration of mobile technology through all strata of society. Mobile technologies including cell phones, tablets, and even some e-readers are used for surfing the web, running apps, reading email, posting to social media, conducting banking transactions, etc. This liberation from desktop and laptop machines and from the requirements of a specific geographic location raises concerns regarding the problems and challenges of maintaining security while traversing cyberspace. The purpose of this empirical study is to investigate the attitudes, behaviors, and security practices of business students using mobile devices to access online resources. One group of students surveyed received no specific training regarding mobile security while a second group was surveyed following the completion of an online training program. Results show no significant difference in the security practices of the two groups, indicating that commercially available security training programs are largely inefficacious with respect to modifying student behavior and that additional research on training efficacy is needed.

Keywords: mobile device, mobile technology, training, higher education.

1. Introduction

The proliferation of mobile technologies has drastically altered societal behavior, where routine tasks are readily performed online using mobile technology rather than through the conventional means of desktop or laptop computing or physical geographical presence. From 2004 through 2015, the growth rate of mobile phone ownership consistently exceeded the combined growth rate of desktop and laptop computer ownership (Pew Internet, 2014). In fact, the convenience of cell phones has resulted in a drastic decline in the existence of landlines (Pew Internet, 2013). Cell phones are not just devices for making phone calls, but rather, they are small computers in themselves. The psycho-

logical impact on consumers of the ubiquity of mobile technology has been one of ready acceptance. Mobile devices are used for sending and receiving texts, for surfing the web, for executing software applications, for engaging in ecommerce, for executing financial transactions (Yoon & Occeña, 2014), and for querying directions to desired destinations. While some of these activities may be innocuous, a potential for a security breach (Zonouoz, Houmansadr, Berthier, Borisov, & Sanders, 2013; Zhao, Zhang, Ge, & Yuan, 2012; van Cleeff, 2008; Wang, Streff, & Sonell, 2012), possibly with devastating consequences, always lurks in the background because, as with desktop computers and laptops, mobile devices are susceptible to multifarious forms of malicious IT infringements.

The ready access to mobile devices combined with the perceived ease of use and significant utility of these devices has resulted in a dutiful acceptance. Since 2004, many smartphone users have reported significant malware attacks (Wang, Streff, & Sonell, 2012; Ingerman, Yang, & EDUCAUSE, 2011; Felt, Finifter, Chin, Hanna, & Wagner, 2011), however, most users are unaware of preventive measures that may be implemented to help thwart nefarious attacks (Paullet & Pinchot, 2014). While concerns for security and privacy of information is present in the minds of most users, these thoughts are generally relegated to obscurity and abandoned or neglected (Gupta, Kumar, & S., 2014) in favor of instant access and immediate gratification for mobile technology has gained firm footing as the dominant medium for conducting business, for education, and for social interaction.

The youthful population at college and university campuses is ungrudgingly receptive to the integration of new technologies and innovative strategies for completing traditional activities. Therefore, mobile technologies enjoy a sound grounding among college students. Given the plethora of mobile devices that are prevalent on college campuses, it is imperative to establish and maintain adherence to proper security protocols. While the student population on college campuses may be the most aggressive in embracing innovative technologies, previous studies have shown that this stratum of the population lacks vigilance in their devotion to security procedures (Jones & Chin, 2015; Jones, Chin, & Aiken, 2014; Jones & Heinrichs, 2012). Appropriate precautions are not necessarily taken and necessary security protocols are not routinely implemented in order to safeguard personal privacy and personal wellbeing. Students insouciantly use their mobile devices to traverse cyberspace.

Mobile security is the new frontier on which the struggle for a secure internet experience will be manifested. It is well documented that information security research is largely technical, largely ignoring the role of the human agents who interact with technology. The current paper is positioned within the broader, emerging stream of behavioral research into information security. Previous studies (Jones & Chin, 2015; Jones, Chin, & Aiken, 2014; Jones & Heinrichs, 2012) have examined the security practices amongst mobile phone users within the most active demographic (college students), however, these studies have not investigated the responsiveness of these practices to security training programs. The current work is a first step in this direction. While some previous studies have advocated general security awareness training as effective mechanisms for protecting individuals and organizations against malicious activity in

an increasingly connected world (Siponen, 2000), there is a tendency in these studies to conceive of success as an increase in awareness. In the present study, we are concerned not just with awareness but also with actual behaviors of college students following the receipt of training. The purpose of the current study, then, is to continue the research stream (Jones & Chin, 2015; Jones, Chin, & Aiken, 2014; Jones & Heinrichs, 2012) on the security behavior of college students when using mobile technologies. Specifically, we investigate the efficacy of general security training with respect to consumer behavior when employing mobile technologies. Our focus is on mobile security, but we are confident that our findings are externally valid with respect to the security of other information systems platforms and paradigms as well.

2. Related Work

2.1. *Unsafe Security Practices*

The extant research literature is consistent in that information security is a major concern (Montesdioca & Macada, 2015) especially given the mass proliferation of mobile devices, and their universal use in accessing sensitive data. A plethora of previous studies (Terzis & Economides, 2011; Padilla-Meléndez, Aguila-Obra, & Garrido-Moreno, 2013) present empirical research that demonstrate a sore lack of compliance with, and even a basic knowledge of, security standards and precautions (Jones & Chin, 2015; Jones, Chin, & Aiken, 2014; Jones & Heinrichs, 2012). Mylonas *et al.* (2013a, 2013b) conducted a survey to assess security awareness of smartphone users who download applications from various application repositories and found that users exhibit a blind trust in such repositories and do not necessarily exercise caution when selecting, downloading, and installing applications. Harris *et al.* (2016a) studied the factors influencing consumers' intent to install mobile applications and concluded that consumers knowingly take unnecessary security risks, which raises "major security and privacy concerns." In another study, Harris *et al.* (2016b) study consumer reaction to excessive permission requests when installing mobile apps and conclude that consumers have become desensitized to security requests and hence the precautions taken by consumers may be inadequate. Mensch and Wilkie (2011) compared security practices of college students and reported a "troubling disconnect" among information security attitudes, behaviors, and tool usage. Harris *et al.* (2014) surveyed college students who are nearing graduation and determined that significant weaknesses exist in security practices, establishing a need for security awareness and training programs. Patten and Harris (2013) proposed integrating mobile security education into the IT curriculum to help educate current students who will become future IT professionals. Jones & Chin (2015) surveyed college students following the ubiquitous saturation of smartphone technology on campus and concluded that the data showed a worrisome trend that clearly elucidates the need for training programs and suggested that students be made more aware of security issues and be taught appropriate precautions. The previous research literature is consistent

in that while students may practice a rudimentary level of mobile security, this level is sorely ineffective against diabolical intentions (Kim, 2014).

As a logical outcome of the aggregation of existing published research on the unsafe security practices of consumers and leveraging the literature on the technology threat avoidance theory (TTAT) that posits that users will execute safeguarding measures in order to avoid perceived threats (Liang & Xue, 2009), a common suggestion that has emerged amongst educators and researchers is to integrate mobile security education and training into education curricula (Patten & Harris, 2013, Jones & Chin, 2015) and into organizational educational programs. The expectation is that with the integration of training programs, mobile device users will become enlightened to omnipresent and lurking dangers and will subsequently modify their behavior and judiciously implement and consistently adhere to sage security practices.

2.2. *Security Training*

A conglomeration of literature exists that is directed at understanding the ways in which individuals respond to information security training. Shaw *et al.* (2009) conduct a lab experiment designed to understand how the richness of information security training impacts perception, comprehension and projection of information security risks or threats. They find significant evidence that the richness of security training (Daft & Lengel, 1986) is strongly related to the above three human responses such that richer training materials would lead to more desirable levels of perception, comprehension and projection of information security risks. Shaw *et al.* (2009) measure their outcomes (i.e. perception, comprehension, and projection) by assessing respondent performance on some researcher-developed test. Cox *et al.* (2001) show that security awareness can be improved by discussion sessions, online tutorials, and checklist approaches. However, this study does not capture the efficacy of security awareness programs with respect to actual security-specific behavior. Others (Thomson & von Solms, 1998) advocate the use of social psychology theory to inform the development of information security awareness programs although there are no empirical tests attesting to the efficacy of these approaches. Another study, Puhakainen and Siponen (2010) design a theoretically grounded security-policy compliance training program informed by the concepts of the elaboration likelihood model (Petty & Cacioppo, 1986) and universal constructive instructional theory (Schott & Driscoll, 2012). Their study follows the tradition of action research such that the researchers propose an intervention in a real organizational setting and observe outcomes that could be tied to their intervention. Specifically, there existed a problem with security policy compliance and the study (Puhakainen & Siponen, 2010) structured a training program that produced favorable results in employee behavior. This study is an example of training resulting in actual behavioral change. However, the training was highly involved and highly specific, addressing one small portion of the broader problem of secure behavior (as measured by policy compliance in this case). In addition, employees are to follow policy as a result of mandate. This is quite different from individuals, college students on their mobile phones, for example, voluntarily adopting secure practices in their everyday lives.

In summary, the prevailing research into information security training fails to acknowledge the difference between awareness and action. Most studies either establish complacency in security practices and advocate training (Jones & Heinrich, 2012, Jones & Chin, 2015) or focus on increasing security awareness as a result of training but fail to analyze the impact of the training on actual behavior (Cox et al, 2001). Further, most studies are couched within the organizational context, evaluating security training by the extent to which employees adhere to a mandated security policy. However, for the demographic of college students that is studied in the present research, compliance is not mandatory. In fact, many institutions of higher education do not even have a clear security policy in place regarding mobile technologies.

The present study extends previous work and contributes to the research literature in that we collect data and provide analysis to gauge alterations in behavior resulting specifically from the implementation of an online training program. This is an extremely important contribution because college students with privately owned technologies are not subjected to mandatory security regulations and practices when using their personal mobile devices. However, these devices are often used to access university resources such as online course systems, financial aid information, registrar data, and email, and therefore, these devices must be appropriately protected. It has become vitally important to gauge the efficacy of training programs on this liberated stratum of society that enjoys largely unrestricted mobile technology use.

3. Research Questions and Methodology

Based on a review of the existing literature, the most frequently recommended security practices for consumers are: (1) avoid harmful behaviors and activities, (2) provide protection through the use of phone settings and/or add-on utilities, and (3) prepare for disaster recovery (Jones & Heinrichs, 2012, Jones & Chin, 2015). In designing our survey, we used the vetted survey of college students from these earlier studies as a baseline, and therefore, no additional pilot study was conducted. For the purpose of the survey design and data analysis, we organized behavior and practices into the same three approaches, as summarized in Table 1 (Jones & Heinrichs, 2012, Jones & Chin, 2015).

Since these previous studies concentrated only on assessing the awareness of college students to security practices and included no component to implement training and assess subsequent behavior, the current study extends these previous studies in that our research considers the approaches in Table 1 with the embedded component of general security training. Specifically, we examine the following research questions:

RQ1. How does the propensity to practice harmful mobile security behaviors respond to general security training?

RQ2. How does the propensity to use device features to provide protection respond to general security training?

RQ3. How does the propensity to use add-on features to provide protection respond to general security training?

Table 1
Security approaches and practices Jones and Heinrichs (2012)

Approach	Practices
Avoid harmful behaviors and activities	Do not apply software updates Click on links in text messages and emails Open email attachments from unknown sources Use phone for financial purposes Download risky third-party applications Download applications requesting access to personal information Connect to unknown networks
Provide protection through phone settings and add-on utilities	Enable encryption Enable password protection Enable lock/timeout for inactivity Disable Bluetooth when not in use Install firewall Install anti-malware Apply remote services: remote lock, remote wipe Disable GPS when not in use
Prepare for 0disaster recovery	Avoid phone loss Immediately report phone loss Record IMEI number Back up data Insure phone

3.1. *Sample and Method*

We divided our participants into two groups and conducted a two-group post-test only quasi-experiment (Campbell, Stanley, & Gage, 1963) with a researcher-controlled intervention (treatment) of a training program administered as several online self-paced modules. Both groups consisted of undergraduate students at a large public university in the southeastern United States. Of the two groups, one received our intervention (n = 187) while the other group did not receive the intervention (n = 160). The two groups were mutually exclusive such that no member of one group was also a member of the other group. The group that did not receive the intervention (untreated) consisted of students enrolled in an introductory course in management information systems in Spring 2014. The group that did receive the intervention (treated) was enrolled in the same course offered in Fall 2014 and in Spring 2015. The same professor taught all three sections of the course. As random assignment was not practically feasible, we operated on the assumption that the two groups were drawn from the same population to the extent that there existed no differences between the two groups that could confound our results. We will show that it can be reasonably assured that the groups were similar along key dimensions likely to confound our dependent variables. This is of critical importance, as differences between the groups ought to be attributable solely to the intervening treatment, the training modules.

The survey was administered online using Qualtrics to a convenience sample of students in all three sections of the course. Students were given instructions via an electronic announcement posted on the course Blackboard sites. These instructions included

a link to participate in the survey, which was accessible online from any location and at any time. Participants responded anonymously to a series of questions and were then redirected to a new website where they could enter basic identifying information so as to receive extra credit points. As in Jones & Heinrichs (2012) and Jones & Chin (2015), the first part of the survey contained six demographic questions and established phone ownership (major, gender, age bracket, year in school, type of cell phone, type of operating system). Participants who did not have a smartphone were instructed to cease participation after answering these initial questions. Only smartphone users were encouraged to continue through Part II of the survey, which asked 22 questions that addressed security awareness and practices.

3.2. *Treatment: Training Program*

Jones and Heinrichs (2012) sought to understand mobile security practices amongst university undergraduates. Jones and Chin (2015) assessed undergraduate students' smartphone security practices in 2014, and compared this behavior to results from the same survey instrument when administered in 2011 in Jones and Heinrichs (2012). Both studies concluded that students continue to exercise risky practices when using their mobile devices. Each of these previous studies suggest that training options should be implemented to educate the population with the hopes that such training programs will provide the necessary enlightenment to encourage safer mobile computing practices. With this in mind, the current work extends these previous works by conducting a study that assesses security behavior in the absence of training and compares these results to the security practices of participants that completed a self-paced training program. Our experiment was designed with the overarching objective of observing mobile security practices after the researcher-controlled intervention of a training program.

A basic series of information security videos produced by the SANS Institute and purchased by the university for security training of the university community were used as the experimental introduced intervention (treatment). These training videos covered areas including mobile security, social networking, password protection and data protection. The videos were made available as online modules and students were allowed to watch the videos multiples times and were encouraged to study the material thoroughly. Upon completion of the training program, students receiving the treatment were required to take an online test for a portion of their course grade. Students completed the training course online and in their own time, such that the researchers controlled neither the timing nor the conditions under which the modules were consumed.

3.3. *Homogeneity of Populations*

In this section, we present our statistical analysis aimed at providing an acceptable level of assurance that the two student treatment groups were homogenous along researcher-determined dimensions. Assurance that groups consisted of individuals from the same

population is essential in ruling the effect of variables other than the intervention on the target constructs. We computed a series of Pearson Chi-Square (χ^2) tests to examine the relationship between group membership (i.e. treated and untreated) and the following variables: college year χ^2 (3, n = 347) = 5.482, p = .140; gender χ^2 (1, n = 347) = .062, p = .803; major χ^2 (9, n = 343) = 20.426, p = .015; age χ^2 (9, n = 347) = 4.432, p = .218; GPA χ^2 (4, n = 347) = 1.183, p = .881; phone type χ^2 (2, n = 347) = 1.478, p = .478; and operating system χ^2 (4, n = 347) = 1.377, p = .848.

With respect to college year, where college year ranged from freshman through to graduate student, we found no statistically significant difference in the distribution of respondents between treatment groups. Similarly, there was no statistically significant difference between groups for gender or for age. Grade point averages were similarly distributed between treatment groups such that no statistically significant difference was found. Regarding respondents' phone type (i.e. smart phone with data enabled, smart phone without a data plan, ordinary phone, and no phone), no significant differences were observed. In the same vein, respondents across groups were similarly distributed with respect to mobile operating system. However, we did observe a statistically significant difference in the distribution of respondents around major academic areas. This difference is largely attributable to the higher proportion of accounting majors in the untreated group (13.8% vs. 3.8%), and the higher proportion of economics majors in the treated group (6% vs 1.3%). The two groups were quite similar across the remaining eight majors listed on the instrument.

We conclude that, based on the results of our tests of group differences, there were no serious threats to the homogeneity of the student experimental groups. However, we cannot rule out several threats to the validity of our experimental results with respect to causal inference. For example, there may be factors that vary significantly between groups that may confound results that we did not identify. Further, we have no means of assessing the extent to which the self-selection of respondents into groups (i.e. respondents register for a course independent of the researchers' control) may impact findings. There may also be threats associated with treatment fidelity as the treatment was administered in a controlled environment. We attempted to ensure that respondents had an adequate grasp of the training materials by administering a test, thus, to some extent, mitigating some of the negative implications of a minimally controlled experimental stimulus.

4. Hypotheses Development Using Factor Analysis

Jones and Heinrichs (2012) and Jones and Chin (2015) posed three broad questions regarding security practices. These questions are termed "approaches" to security in their paper and are as follows: avoid harmful behaviors and activities, provide protection through phone settings and add-on utilities, and prepare for disaster recovery. Each approach subsumes several security practices as detailed in Table 1. While we use Jones and Heinrichs' (2012) and Jones and Chin (2015) works as a starting point, we do not follow them in lockstep. We retain only the approaches and the corresponding practices

that could be affected by our experimental intervention and only those practices that were confirmed as congruent with their corresponding approach by a factor analysis. Based on the results of our factor analysis and our concerns with the ability of approaches to be affected by the experimental stimuli, we have derived new approaches while eliminating others.

Each of the security practices identified in Table 1 maps to a similarly worded question in the Jones and Heinrichs (2012) survey instrument that has been replicated for our purposes. In our three research questions, we sought to confirm that the security practices listed were actually components or dimensions of an individual's propensity towards an approach. For example, do the following practices – application of software updates, clicking on text message and email links, downloading third party applications and connecting to unknown networks – capture aspects of the individual's propensity to avoid harmful behaviors and activities when using a mobile device? A large number of items from the Jones and Heinrichs (2012) survey instrument were not appropriate for the multivariate analysis of variance (MANOVA) procedure suited to our purposes. We required a process to systematically reduce the number of items in the Jones and Heinrich (2012) instrument. Further, we elected to focus our analysis on our three research questions. We excluded the Jones and Heinrichs' (2012) third approach, "prepare for disaster recovery," as we did not believe it to be sensitive to our stimulus. Accordingly, as shown in Table 2, we used two of the original Jones and Heinrichs (2012) approaches and added a third approach, while, for the moment, maintaining the full list of practices.

In order to reduce the number of dependent variables, we employed a principal components factor analysis to discover the natural groupings of the security practices into security approaches and to eliminate the redundant variables. Our analysis did not use the factor scores obtained, but rather, relied on the technique to select only those prac-

Table 2

Results of Principal Components Factor Analysis Aligning Approaches and Practices

Practices	Approaches		
	Avoid Harmful Behaviors and Activities	Use Add-on Features to Provide Protection	Use Built-In Features to Provide Protection
Open email attachments from unknown sources	.627	-.169	.060
Click on links in text messages and emails	.651	-.222	.164
Use phone for financial purposes	.492	.056	-.106
Download risky third party applications	.624	-.031	.049
Download applications requesting access to personal information	.636	.177	-.153
Disable Bluetooth when not in use	.012	-.172	.775
Disable GPS when not in use	.066	.123	.759
Connect to unknown Wi-Fi networks	-.085	.216	.428
Install and enable anti-malware (anti-virus)	.042	.838	.149
Install and enable encryption software	-.113	.823	.009

tices which load into our selected approaches and those which contribute well to the overall factor solution as assessed by communalities. Based on these factor loadings and communalities, we calculated Cronbach's alpha (Cronbach, 1951) to describe how well a group of practices focuses on a single approach. The results of our factor analysis and associated alphas are shown in Table 2 and in Table 3.

With the exception of the "Use Add-on Features to Provide Protection" approach to mobile information security, Cronbach's alphas are generally low for our data. However, we deem these figures acceptable as our purpose here is not to find dimensions (practices) that underlie constructs (approaches) but to systematically ascertain general questions which may be answered using the Jones and Heinrichs (2012) instrument by finding natural groupings of mobile security practices. An added benefit to this approach is that it structures well with the multivariate analyses of variance, which we will use to test our three research questions.

Several researchers lend support to the notion that training programs may abet in improving the security behavior of mobile users. Harris *et al.* (2014) and He (2013) suggest implementing mobile device security awareness and training for users while Slusky and Partow-Navid (2012) suggest user awareness training that links knowledge with practice. Furthermore, these training exercises should be administered frequently over time as a reminder of safe practices and in order to effectively incorporate contemporary technologies. Therefore, using the research questions developed in the preceding section, we construct our associated hypotheses as shown in Table 4. We hypothesize that the intervention of a training program will alert participants to impending dangers and

Table 3
Unstandardized and Standardized Cronbach's Alphas

	Unstandardized Cronbach's Alpha	Standardized Cronbach's Alpha
Avoid Harmful Behaviors and Activities	0.542	0.577
Use Add-on Features to Provide Protection	0.661	0.669
Use Built-in Features to Provide Protection	0.436	0.426

Table 4
Research Questions and Hypotheses

Research Question	Hypothesis
How does the propensity to practice harmful mobile security behaviors respond to general security training?	H1 *The propensity to practice harmful mobile security behaviors will be decreased as a result of general security training.*
How does the propensity to use device features to provide protection respond to general security training?	H2 *The propensity to use device features to provide protection will be increased as a result of general security training.*
How does the propensity to use add-on features to provide protection respond to general security training?	H3 *The propensity to use add-on features to provide protection will be increased as a result of general security training.*

based on the tenets of the technology threat avoidance theory (Liang & Xue, 2009), will decrease harmful security behavior while increasing the use of device features and the use of add-on features to increase security protection of mobile devices.

To test each of our hypotheses, we leverage the strength of MANOVA by asking what Hair *et al.* term as intrinsically multivariate questions (Montesdioca & Macada, 2015; Hair, Black, Babin, Anderson, & Tatham, 2006). MANOVA allows for the creation of linear combinations of multiple dependent variables (a variate) against which the univariate analysis of variance procedure is conducted (ANOVA). We build three separate MANOVAs, one for each experimental hypothesis.

We retain the original scales from Jones and Heinrichs' (2012) work, where each security practice is measured on a 3-point scale. The Jones and Heinrichs (2012) scales all ranged from 1–3, 1 = yes or always, 2 = maybe or sometimes, 3 = no or never. This becomes quite problematic. Take as examples the following two questions: 1. "Have you or would you open a multimedia attachment (e.g. pictures, video, audio) received in a text or email from an unknown source?" 2. "Do you disable Bluetooth when it's not in use?" Both questions are scaled as shown above. However, a score of 3 in the first question indicates a desirable behavior, while a score of 3 on the second question indicates an undesirable behavior. Therefore, we recode the data obtained from the survey instrument to ensure a consistent analysis. That is, a score of 3 always indicates a desirable behavior, a score of 2 a neutral behavior, and a score of 1 indicates an undesirable behavior.

5. Results

To test H1, a MANOVA model is constructed with the following security practices as dependent variables: open email attachments from unknown sources, click on links in text messages and emails, use phone for financial purposes, download risky third party applications and download applications requesting access to personal information. The independent variable is categorical and captures whether or not a respondent participated in the treatment. There is a statistically significant difference in the propensity to practice harmful mobile security behaviors depending on whether or not a respondent received the treatment, F (5, n = 342) = 27.158, $p < .001$; Wilk's $\Lambda = .712$, Partial $\eta^2 = .288$. Further, the treatment had a statistically significant effect on the propensities to: open email attachments from unknown sources (F (1, n = 342) = 16.27; $p < .001$, partial $\eta^2 = .046$), click on links in text messages and emails (F (1, n = 342) = 17.663; $p < .001$, partial $\eta^2 = .049$), use phone for financial purposes (F (1, n = 342) = 22.852; $p < .001$, partial $\eta^2 = .063$), download risky third party applications (F (1, n = 342) = 25.563; $p < .001$, partial $\eta^2 = .070$), and download applications requesting access to personal information (F (1, n = 342) = 105.859; $p < .001$, partial $\eta^2 = .237$). However, the data did not meet a key assumption of MANOVA, that is, the equality of variance covariance matrices between groups. Common tests of this assumption, Box's M and Levene's test of homogeneity of variance, both resulted in the rejection of the null hypotheses that variance-covariance matrices are equal between groups and that variance is homogenous

between groups respectively. We present the mean scores in Table 5 with this caveat. From Table 5, we find that we are unable to lend support to our hypothesis. Respondents receiving the treatment had a higher tendency towards risky security behavior, running counter to our hypothetical prediction (recall that the higher the score, the more desirable the behavior).

We ran a separate multivariate analysis of variance to test the second hypothesis (H2), that the propensity to use device features to provide protection will be increased as a result of general security training. We use as dependent variables in this MANOVA, respondent's propensities to disable Bluetooth when not in use, disable GPS when not in use and connect to unknown Wi-Fi networks. The independent variable is categorical and captures whether or not a respondent participated in the treatment. We found no statistically significant difference between treatment groups on these dependent variables. Results of the omnibus MANOVA are F (3, n = 344) = .748, p = .524; Wilk's Λ = .993, Partial η^2 = .007. In addition, the treatment did not have statistically significant effects on respondents propensity to: disable Bluetooth when not in use (F (1, n = 344) = .554; p = .457, partial η^2 = .002), disable GPS when not in use (F (1, n = 344) = .132; p = .717, partial $\eta^2 < .000$), and connect to unknown Wi-Fi networks (F (1, n = 344) = .900; p = .174, partial η^2 = .005). Table 6 summarizes the mean differences on these three dependent variables between treatment conditions.

Table 5
Between Group Means – Practice Harmful Security Behaviors

Treatment		Mean	Std. Deviation	N
Open email attachments from unknown sources	Untreated	2.89	.473	158
	Treated	2.65	.627	184
Click on links in text messages and emails	Untreated	2.97	.346	158
	Treated	2.77	.493	184
Download risky third party applications	Untreated	2.91	.489	158
	Treated	2.58	.664	184
Use phone for financial purposes	Untreated	1.94	1.001	158
	Treated	1.51	.627	184
Download application requesting access to personal information	Untreated	2.78	.674	158
	Treated	2.03	.673	184

Table 6
Between Group Means – Use device features to provide protection

Treatment		Mean	Std. Deviation	N
Disable Bluetooth when not in use	Untreated	2.46	.834	158
	Treated	2.53	.779	186
Disable GPS when not in use	Untreated	2.28	.822	158
	Treated	2.32	.826	186
Connect to unknown Wi-Fi networks	Untreated	2.25	.684	158
	Treated	2.35	.706	186

Table 7
Between Group Means – Use add-on features to provide protection

Treatment		Mean	Std. Deviation	N
Install and use anti-virus software	Untreated	1.38	.718	159
	Treated	1.48	.785	187
Install and use encryption software	Untreated	1.28	.594	159
	Treated	1.31	.639	187

Finally we test the third hypothesis (H3) that the propensity to use add-on features to provide protection will be increased as a result of general security training. We use as dependent variables in a MANOVA the use of anti-malware and the use of anti-virus software. The independent variable groups responses into those who received training and those who did not (treated and untreated). Results of the omnibus MANOVA indicate that we were unable to detect any statistically significant difference on the propensity to use add-on features to provide protection between individuals who received general security training and individuals who did not: F (2, n = 344) = .738, p = .479; Wilk's Λ = .996, Partial η^2 = .004. With respect to the use of anti-virus software we find that the treatment did not have a statistically significant effect (F (1, n = 344) = 1.466; p = .227, partial η^2 = .004). The use of encryption software was also statistically unaffected by the training program (F (1, n = 344) = .251; p = .617, partial η^2 = .001). Table 7 summarizes the means between the treatment groups.

6. Summary and Conclusions

Jones and Chin (2015) clearly established the ubiquitous penetration of mobile technology amongst business undergraduates at a public institution of higher education, a stratum of society characterized as prolific adopters of current technologies. The security of these unregulated mobile devices has become of paramount importance, for these devices are routinely used for accessing university servers and systems including email, Blackboard, online testing servers, student information systems, financial aid systems, and grade systems. Earlier studies (Jones & Chin, 2015, Harris *et al.*, 2016a, Harris *et al.*, 2016b, Patten & Harris, 2013) have indisputably established a lack of appropriate security practices by these users and have suggested the institutionalization of security training programs with the hopes of altering the lackadaisical behavior in favor of a conscientious adherence to security protocols. The current research is a step in this direction.

The purpose of the current research was to gauge the efficacy of general security training on the mobile security practices of college students. Our experimental procedure was structured in such a way that the only difference pertinent to mobile security practices between the two groups of students was that one class received the training

program and the other did not. Drawing from self-determination theory (SDT), which suggests that people are intrinsically motivated to pursue self-fulfillment in personal areas of interest and where exists at least a perception of high competence (Deci & Ryan, 1985), we optimistically hypothesized that mandated training would have a positive impact across our three areas of concern (harmful behaviors, use of device features, use of add-on features) in that harmful mobile security behaviors would decrease as a result of security training, which would promote a sense of knowledge and empowerment. The group of students that completed the general security training program (the intervention) did demonstrate learning on some practices and consequently, some improvement in behavior; however, this change was statistically insignificant. Using quantitative data and analyses, our study confirms that student behavior with regard to mobile security practices continues to be liberal, with or without participation in a commercially available training program.

To help explain the indifferent attitude toward mobile security, even following a self-paced, mandatory training program, we turn to Shepherd and Kay (2012) and their theory of motivated avoidance of sociopolitical information. While this theory has never before been applied in the domain of mobile security, we foresee great potential in their theoretical propositions to explain the psychological inclinations of complacency toward mobile security. The Shepherd and Kay (2012) model describes a behavioral path beginning with a "psychological discomfort associated with epistemic uncertainty." Securing one's information is a technically challenging endeavor, if for no other reason, then because a deluge of information is available on the matter. The situation is further complicated by the multiplicity of mobile computing platforms and their almost perpetual evolution. Securing one's mobile device may readily be described as a complex activity, where such activities lead individuals to "simply outsource personal responsibility to supposed qualified others" (Shepherd & Kay, 2012). It may, in this manner, seem reasonable to us to trust our device manufacturers and software companies to fortify our devices against attack. As such, our increasing dependence on device manufacturers, software vendors and government agencies to guarantee our security leads us from dependence on these entities to a psychological acceptance of blind trust in these entities and a convenient relinquishment of individual duty for ensuring safety when using mobile devices.

We argue, using Shepherd and Kay's (2012) insight, that higher levels of trust in device manufacturers, software companies and the government agencies charged with their regulation, temper the effect of increased security awareness on actual security behavior. Shepherd and Kay (2012), invoking cognitive dissonance theory, argue that "to the extent that people increasingly trust or justify the legitimacy of an authority to cope with their dependence on it, they should be motivated to avoid information that could potentially rupture this trust" (Shepherd & Kay, 2012). We argue that trust not only leads to information avoidance, but inaction as well. This is consistent with the results of our study, which indicate that instituting a training program may not provide sufficient impetus to alter the ingrained apathy and the delegation of responsibility for security. Certainly, our findings hint at the need to study how efficacious training programs may be made available in a cost effective, efficient manner.

Our study is an initial empirical exploration that has called into question the usefulness of general security training, in the form of training videos, in changing the security behavior of college students. Earlier studies such as Hansche (2001) have advocated more hands-on approaches for security education. Hansche (2001) classifies as security awareness the sort of intervention presented herein. She classifies as training a more involved approach to security that involves active working sessions similar to those used to great effect in Puhakainen and Siponen (2010). However such involved training approaches are not always feasible, especially for a large public institution with thousands of staff and faculty, and over thirty thousand students.

In light of our results, charting a path for future research is of paramount importance. One future research direction is to conduct this study using a larger sample size that may strengthen some of the insignificant relationships to the point of significance. Additionally, a sample could be collected from a more diverse group, such as students from different concentrations of study and from different universities. Other sectors of the population, such as university faculty and administrators, IT and other professionals, may also be surveyed, as security concerns on mobile devices affect all of these constituencies. In repeated trials of this research, an additional suggestion for improvement is to employ a seven, nine, or ten point Likert scale rather than the five-point scale employed in the present study. Through statistical testing comparing rating scales, research has shown that seven, nine, and ten point scales are preferable (Preston and Colman, 2000). Finally, another research direction is to test the efficacy of different training programs and furthermore, using the current study as a benchmark, to gauge the potency of systematic and repeated exposure to security training. Frequent exposure may lead to repeated awareness and encourage behavioral modification.

References

Campbell, D.T., Stanley, J.C., Gage, N.L. (1963). *Experimental and quasi-experimental designs for research*.

Cox, A., Connolly, S., Currall, J. (2001). Raising information security awareness in the academic setting. *VINE*, 31(2), 11–16. http://doi.org/10.1108/03055720010803961

Cronbach, L.J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika,* 16, 297–333.

Daft, R., Lengel, R. (1986). Organizational information requirements, media richness and structural design. *Management Science*, 32(5). Retrieved from: http://pubsonline.informs.org/doi/abs/10.1287/mnsc.32.5.554

Deci, E.L., Ryan, R.M. (1985). *Intrinsic Motivation and Self-Determination in Human Behaviour*. New York: Plenum.

Felt, A., Finifter, M., Chin, E., Hanna, S., Wagner, D. (2011). A survey of mobile malware in the wild. In: *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*. 3–13.

Gupta, K., R. Kumar, and S. Loothra. (2014). Smartphone security and contact synchronization. In: *Proceedings from CSNT 2014: Fourth International Conference on Communication Systems and Network Technologies*. 621–625. Retrieved from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6821472&isnumber=6821334. http://dx.doi.org/10.1109/CSNT.2014.130

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., Tatham, R.L. (2006). *Multivariate Data Analysis* (Vol. 6). Pearson Prentice Hall Upper Saddle River, NJ.

Hansche, S. (2001). Designing a security awareness program: Part I. *Information Systems Security*, 9(6), 14. Retrieved from: http://proxy.library.vcu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,url,cookie,uid&db=a9h&AN=3943159&site=ehost-live&scope=site

Harris, M.A., Brookshire, R., Chin, A.G. (2016a). Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management*, 36(3). http://dx.doi.org/10.1016/j.ijinfomgt.2016.02.004.

Harris, M.A., Chin, A.G., and Brookshire, R. (2016b) Mobile app installation: the role of precautions and desensitization, *Journal of International Technology and Information Management*, 24(4). http://scholarworks.lib.csusb.edu/jitim/vol24/iss4/3

Harris, M.A., Furnell, S., Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy & Security,* 10(4), 186–202. Retrieved from: http://proxy.library.vcu.edu/login?url=http://search.proquest.com.proxy.library.vcu.edu/docview/1691007848?accountid=14780

He, W. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management & Computer Security*, 21(5), 381–400.

Ingerman, B., Yang, C., EDUCAUSE Current Issues Committee (2011). *Top-Ten It Issues*, 2011. Retrieved from: http://www.educause.edu/ero/article/top-ten-it-issues-2011

Jones, B., Heinrichs, L. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems,* 53(2), 22–30. Retrieved from: http://iacis.org/jcis/articles/JCIS53-2-3.pdf

Jones, B. and Chin, A., (2015). On the efficacy of smartphone security: a critical analysis of modifications in business students' practices over time. *International Journal of Information Management*, 35(5), 561–571. http://dx.doi.org/10.1016/j.ijinfomgt.2015.06.003

Jones, B., Chin, A., Aiken, P. (2014). Risky business: students and smartphones. *TechTrends*, 58(6), 73–83. http://dx.doi.org/10.1007/s11528-014-0806-x

Kim, E. (2014). Recommendations for information security awareness training for college students. *Information Management and Computer Security*, 22(1), 115–126. DOI: http://dx.doi.org/10.1108/IMCS-01-2013-0005.

Liang, H., Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly*, 33(1), 71–90.

Mensch, S., Wilkie, L. (2011). Information security activities of college students: an exploratory study. *Academy of Information and Management Sciences Journal*, 14(2), 91–116.

Montesdioca, G., Macada, A. (2015). Measuring user satisfaction with information security practices. *Computers & Security,* 48, 267–280. DOI: 10.1016/j.cose.2014.10.015

Mylonas, A., Kastania, A., Gritzalis, D. (2013a). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, 47–66.

Mylonas, A., Meletiadis, V., Mitrou, L., Gritzalis, D. (2013b). Smartphone sensor data as digital evidence. *Computers & Security*, 38, 51–75.

Padilla-Meléndez, A., Aguila-Obra, A.R., Garrido-Moreno, A. (2013). Perceived playfulness, gender differences and technology acceptance model in a blended learning scenario. *Computers & Education,* 63, 306–317. DOI: 10.1016/j.compedu.2012.12.014

Patten, Karen P.; Harris, Mark A. (2013). The need to address mobile device security in the higher education it curriculum. *Journal of Information Systems Education*, 24(1), 41–52.

Paullet,, K., Pinchot, J. (2014). Mobile malware: coming to a smartphone near you? *Issues in Information Systems*, 15(2), 116–123.

Petty, R.E., Cacioppo, J.T. (1986). The elaboration likelihood model of persuasion. In: *Communication and persuasion* (1–24). Springer.

Pew Research Center Internet Project Survey. (2014). *Mobile Technology Fact Sheet*. Retrieved from: http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/

Pew Research Center Internet Project Survey. (2013*). Cell Phone Ownership Hits 91% of Adults*. Retrieved from: http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/

Preston, C., Colman, A. (2000). Optimal number of response categories in rating scales: reliability, validity, discriminating power, and respondent preferences. *Acta Psychologica*, 104, 1–15.

Puhakainen, P., Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, 34(4), 757–778. Retrieved from: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2933&context=misq

Schott, F., Driscoll, M.P. (2012). On the architectonics of instructional theory. *Instructional Design: International Perspectives: Volume I: Theory, Research, and Models: Volume II: Solving Instructional Design Problems*, 135.

Shaw, R.S., Chen, C.C., Harris, A.L., Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92–100. http://doi.org/10.1016/j.compedu.2008.06.011

Shepherd, S., Kay, A.C. (2012). On the perpetuation of ignorance: system dependence, system justification, and the motivated avoidance of sociopolitical information. *Journal of Personality and Social Psychology*, 102(2), 264.

Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31–41. http://doi.org/10.1108/09685220010371394

Slusky, L., Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy & Security*, 8(4), 3–26.

Terzis, V., Economides, A.A. (2011). Computer based assessment: Gender differences in perceptions and acceptance. *Computers in Human Behavior,* 27(6), 2108–2122. DOI: 10.1016/j.chb.2011.06.005

Thomson, M.E., von Solms, R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security*, 6(4), 167–173. http://doi.org/10.1108/09685229810227649

van Cleeff, A. (2008). Future Consumer Mobile Phone Security: A Case Study Using the Data-centric Security Model. Information Security Technical Report ISSN 1363–4127, 13(3), 112–117. http://www.sciencedirect.com/science/article/pii/S1363412708000460

Wang, Y., Streff, K., Sonell, R. (2012). Smartphone security challenges. *Computer*, 45(12), 52–58. http://doi.ieeecomputersociety.org/10.1109/MC.2012.288

Yoon, H.S. and Occeña, L. (2014). Impacts of customers' perceptions on internet banking use with a smart phone. *Journal of Computer Information Systems*, 54(3), 1–9.

Zhao, M., Zhang, T., Ge, F., Yuan, Z. (2012). RobotDroid: a lightweight malware detection framework on smartphones. *Journal of Networks*, 7(4). http://dx.doi.org/10.4304/jnw.7.4.715-722

Zonouoz, S., Houmansadr, A., Berthier, R., Borisov, N., Sanders, W. (2013). Secloud: a cloud-based comprehensive and lightweight security solution for smartphones. *Computers & Security*, 37, 215–227. http://dx.doi.org/ 10.1016/j.cose.2013.02.002

A. Goyal Chin is an Associate Professor in the Information Systems Department at Virginia Commonwealth University. She received her B.S. in computer science and M.S. and Ph.D. in information systems, all from the University of Maryland at College Park. Her current research interests include data management and mobile and online security. Her research has appeared in the Communications of the ACM, International Journal of Information Management, Journal of Computer Information Systems, Journal of Database Management, Journal of Management Systems, and others.

U. Etudo is a doctoral candidate in the Department of Information Systems at Virginia Commonwealth University. He received his M.S. in Information Systems from Virginia Commonwealth University in 2013. His research interests include text mining, decision support systems, semantic technologies and socio-technical systems. His research has appeared in Decision Support Systems, the proceedings of the Hawaii International Conference on Systems Sciences (HICSS) and the International Conference on Information Systems (ICIS).

M.A. Harris is an assistant professor in the Cyber Institute and College of Business at Augusta University. He has a Ph.D. in Information Systems from Virginia Commonwealth University, a MS in E-commerce and a B.S. in Information Technology from Old Dominion University. His research interests include mobile device security, behavioral factors of security, security policy manage- ment, awareness training, and health IT security. He has authored multiple papers in well-respected refereed information systems journals and conferences. Before aca- demia, Mark was a senior network engineer for a large university, where he oversaw an expansive computer network.