International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2021, Vol. 17, Issue 3, pp. 57-80

A Comparative Analysis of Smartphone Security Behaviors and Practices

Amita Chin
Virginia Commonwealth University, United States

Beth Jones
Western Carolina University, United States

Philip Little
Coastal Carolina University, United States

ABSTRACT

This study on smartphone security behaviors and practices is a continuation of the work in Jones and Chin (2015), where results of a 2011 student survey at a regional comprehensive university were compared to results from a 2014 survey at the same institution. That study found that students continued to be lax in their mobile security practices. In December 2019, we again surveyed undergraduate business students to determine their current level of awareness, attitudes, and security-related practices. In this current study, we compare and contrast the results of our 2019 survey to those from our 2014 administration of the same survey instrument (Jones & Chin, 2015). Our findings help us to clearly identify the specific areas where security behaviors have improved and pinpoint those areas where necessary precautions are still lacking. We believe that our results will prove useful in developing educational programs and in providing training on proper smartphone security protocols.

Keywords: *smartphone security; business students; mobile devices; cell phones*

INTRODUCTION

The ownership and use of mobile devices, including smartphones, tablets, gaming consoles, and e-readers has increased so rapidly in recent years that perhaps no prior technology has ever been more expediently and more ubiquitously accepted by consumers. Using mobile technologies has transformed our personal and professional lives in an unprecedented manner. Smartphones in particular, in combination with the plethora of apps that are readily available for them (Harris, Chin, & Brookshire, 2015), have become wholly integrated into our everyday life. From 2004 through 2015, the growth rate of mobile phone ownership consistently exceeded the combined growth rate of desktop and laptop computer ownership (*Mobile Fact Sheet*, 2019). According to a 2011 Pew study, some 35% of American adults owned a smartphone (Smith, 2011). Just a few years later, in 2014, it was estimated that 55% of the U.S. population owned a smartphone (*Mobile Fact Sheet*, 2019) and by 2019, the number of smartphone users in the United States surpassed 266 million, a staggering 81% of the population (*Mobile Fact Sheet*, 2019). In 2020, at 14 billion, the number of mobile devices in use exceeds the number of people in the world, which is approximately 7 billion (*Current World Population*, 2020), a 2:1 ratio. Going forward, the number of mobile devices is expected to increase to 14.91 billion by 2021 and to 17.72 billion by 2024 (O'Dea, 2020). As their prevalence has increased, smartphones have become more prone to cyberattacks and are associated with a higher level of security risk (Ameen et al., 2021).

Smartphones are not just devices for making phone calls, but rather, they are powerful computers that allow consumers to send and receive texts, surf the web, execute software applications, engage in ecommerce (Chin et al., 2021; Harris, Chin, & Beasley, 2019) and execute banking and investment transactions (Yoon & Occeña, 2014). They even provide built-in cameras and have full GPS functionality. In fact, in 2020, more than half of all of the traffic on the Internet has been originating from a mobile device (Chaffey, 2020). The ready access to mobile devices combined with the perceived ease of use and widespread utility of these devices has resulted in a dutiful acceptance.

The commonplace use of smartphones for a voluminous variety of tasks, the plethora of personal data that is routinely stored on them, and the fact that they are almost always in the possession of the user, almost as if an additional appendage, has given rise to significant security concerns (Stylios et al., 2021). A willy-nilly user adherence to security protocols has incentivized hackers to target smartphones with mobile malware, and such attacks have continued to rise in 2019 (Palmer, 2019). For example, smartphones may allow GPS, Bluetooth, or WiFi tracking of individual movements (Breitinger, Tully-Doyle, & Hassenfeldt, 2020) or may be hacked to access a repository of vast personal data, including address information, contacts, appointments, bank information, and passwords. While biometric security precautions such as faceID (Robertson, Kramer, & Burton, 2015), iris recognition (Elrefaei et al., 2018; Stylios et al., 2021), or gait characteristics (Damaševičius et al., 2016) may thwart some unauthorized physical access, a host of additional security infractions may occur, resulting in an unsanctioned relinquishing of personal data.

The purpose of this study is to extend our previous work (Jones & Chin, 2015) and continue our examination of the attitudes and efficacy of smartphone security behaviors of college students, with a particular focus on amendments, if any, in the security behavior of smartphone users over time. Our initial studies, which surveyed undergraduate business students in 2011 and again in 2014, revealed a disconcerting lack of awareness or care regarding smartphone security. In December 2019, we again surveyed undergraduate business students to determine their current level of awareness, attitudes, and security-related practices. We present the results of our current survey and then compare and contrast these results to those from our 2014 administration of the same survey instrument (Jones & Chin, 2015) for it has become vitally important to protect user information and systems from the possibility of security attacks (Kim, 2014). Our findings help us to clearly identify the specific areas where security behaviors have improved and pinpoint those areas where necessary precautions are still lacking. We believe that our results will prove useful in developing educational programs and in providing training on proper smartphone security protocols (Chin, Etudo, et al., 2016).

The remainder of this paper is organized as follows. Following a review of the previous research literature regarding smartphone usage and security precautions, we present the details of our research methodology and enumerate our research questions. This is followed by an explanation of our research findings and a discussion of their implications. Finally, we identify some limitations of our study and offer several suggestions for future research in this area.

LITERATURE REVIEW

Previous research literature stresses information security as a major concern (Mi et al., 2020; Montesdioca & Maçada, 2015; Talal et al., 2019) especially given the widespread use of mobile devices, and their readily accepted use in storing and accessing sensitive data. For example, in the midst of the COVID-19 pandemic, smartphones and other mobile devices are routinely being used for confidential data storage and interactions including healthcare (Farshidfar & Hamedani, 2020; Ganesh et al., 2020; Sansom-Daly & Bradford, 2020; Zhao et al., 2018) and telehealth services. While there is a strong relationship between perceived risk and precautionary behavior (Siponen, Pahnila and Mahmood, 2006), several previous studies (Das & Khan, 2016; Padilla-Meléndez et al., 2013; Terzis & Economides, 2011) present empirical research that demonstrates a sore lack of compliance with, and even a basic knowledge of, security standards and precautions

(Jones, Chin, & Aiken, 2014; Jones & Chin, 2015; Jones & Heinrichs, 2012; Shah & Agarwal, 2020; Yazdanmehr, Wang, & Yang, 2020). It has been clearly established that the weakest link in maintaining information security is the human user (Shah & Agarwal, 2020). Mylonas et al. (2013; Mylonas, Meletiadis, et al., 2013) conducted a survey to assess security awareness of smartphone users who download applications from the various application repositories such as Google Play and Apple's App Store, and found that users exhibit a blind trust in such repositories and do not necessarily exercise caution when selecting, downloading, and installing applications. Das and Khan (2016) surveyed 500 smartphone users representing three major operating systems and concluded that most users routinely ignore warning messages and are happily unencumbered by security protocols. Harris, Brookshire and Chin (2016) studied the factors influencing consumers' intent to install mobile applications and concluded that consumers knowingly take unnecessary security risks, leading to major concerns about security and privacy. In another study, Harris, Brookshire and Chin (2016) examined consumer reaction to excessive permission requests when installing mobile apps and concluded that consumers have become desensitized to security requests and hence the precautions taken by consumers is often inadequate.

Unsecured mobile devices put both organizations and individuals, both males and females, at risk (Park, Yi, & Jeong, 2014). Hart-Davis (2010) points out, "Go into pretty much any company or organization today, and you'll find people using iPads and iPhones to get their jobs done" (p. xxi). Breitinger, Tully-Doyle and Hassenfeldt (2020) found that while many users are employing lock screens for protection of their devices, these same consumers are disregarding other security best practices, including when connecting to a public Wi-Fi. He and Freeman (2010) show that males are generally more confident using technology than females, possibly because females are nurtured in a manner that is not conducive to self-confidence and self-efficacy beliefs (Zeldin, Britner, & Pajares, 2008; Zhou et al., 2020) even though previous studies have shown a positive association between self-efficacy and behavior (Das & Khan, 2016; Verkijika, 2018; Zhou et al., 2020). Females seem to have a higher usage of smartphones than their male counterparts (Nayak, 2018), however, they are less aware of security threats than males (Johnson & Koch, 2006). While gender differences are present when evaluating smartphone security behavior of employees, in their study of gender differences, Ameen et al. (2020) conclude that most employees, regardless of gender, are unaware of the security risks of using smartphones.

Given the undeniable explosion and rapid proliferation of smartphones and other mobile devices coupled with their persistent, commonplace use, organizations must exercise vigilance in mobile device security (Bitton et al., 2018). This necessity envelops not only commercial enterprises, but also institutions of higher education, which are a stomping ground for a nomadic population of fearless and voracious consumers of bleeding edge technology. College campuses face a challenging dilemma: Institutions of higher education pose increased temptation and increased security risk, for these institutions possess a large volume and variety of sensitive information on a wide range of individuals, and demands for this information are growing (Cate, 2006). Mobile devices, particularly smartphones, inarguably have a powerful and significant presence on campuses and are used for social interaction (Gikas & Grant, 2013) and other entertainment (Amez & Baert, 2020), and also increasingly so for access to academic material, submission of work, online research, and for financial transactions (Felisoni & Godoi, 2018; Nayak, 2018). Technology has become so pervasive and integrated into curriculum that using electronic devices is essential for access to academic resources such as Learning Management Systems and online coursework, particularly since curricula in higher education are increasingly incorporating new methods of teaching and learning that are based on mobile access (Minaie, 2011), including collaborative and open learning (Liao et al., 2016). This level of amalgamation of technology and instruction has been shown to be vital to learning and comprehension. The Campus-Class-Technology (CCT) Theory, for example, attempts to explain the relationships between student engagement and technology theoretically (Gunuc & Kuzu, 2015). In particular, does the infusion of technology into the learning process enhance student interest and involvement, and therefore, yield more effective learning? Gunuc and Kuzu (2015) conducted an empirical study to test the CCT theory and determine the influence of technology on student engagement. They concluded that the use of technology such as laptop, Internet, tablet PC, interactive whiteboard, smartphone, and slideware presentations, in class and out of class increased student engagement. Another study explored the role of mobile technology for mobile learning in higher education and concluded that mobile technology can complement and add value to the current learning models (Motiwalla, 2007). Smartphones are also becoming integrated during class sessions (I. Kim et al., 2019) in the hopes of promoting interactive learning. Smartphones, even more so than desktop PCs (Wong et al., 2015), are used for surfing on and interacting with websites, where a variety of security breaches including cross-site scripting (Hydara et al., 2015; Johns, 2014) can occur. Amez and Baert (2020) provide a systematic review of the previously published literature linking smartphone use and academic success.

Mobile devices now dominate the technology landscape and we must prevail in our struggle for secure usage. Despite the substantial security hazards associated with the massive exposure of personally owned mobile devices, colleges are abound with students employing such technological gadgetry for daily activities and all the while, being remiss in their security practices, (Jones, Chin, & Aiken, 2014; Jones & Heinrichs, 2012; Kim, 2014; Mensch & Wilkie, 2011; Padilla-Melendez, Aguila-Obra, & Garrido-Moreno, 2013; Shah & Agarwal, 2020; Shropshire et al., 2015) and in the online exposure of personal privacy (Furnell & Phippen, 2012; Harris, Brookshire, & Chin, 2016; Harris & Chin, 2016; Kelly, 2018; Marett et al., 2015; Wu et al., 2012). To more accurately gauge the smartphone security practices of college students and to determine the potency of these practices, several researchers have employed survey instruments and analyzed the data (Mylonas, Kastania, & Gritzalis, 2013; Mylonas, Meletiadis, et al., 2013; Padilla-Melendez, Aguila-Obra, & Garrido-Moreno, 2013; Terzis & Economides, 2011). Mensch and Wilkie (2011) compared security practices of college students and reported what was termed a “troubling disconnect” among information security attitudes, behaviors, and tool usage. Nowrin and Bawden (2018) surveyed 356 students in Bangladesh and found that students do not behave securely, some of which is attributable to gender differences. Kim (2014) implemented a survey instrument to gauge the security awareness of college students and concluded that additional security awareness training is needed. 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. Harris, Furnell and Patten (2014) surveyed college students who are nearing graduation and were about to enter the workforce, as well as current IT professionals, and determined that significant weaknesses exist in security practices, further 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. Mi et al. (2020) surveyed 192 students and concluded that motivational interventions might help improve smartphone security behaviors. The previous research literature is consistent in that while students practice a rudimentary level of mobile security, this level is sorely ineffective against diabolical intentions (Kim, 2014).

The present study is a continuation of the work in Jones and Chin (2015), where survey results were collected from 218 undergraduate business students at a regional public university. The study found that students were lax in their mobile security practices, with males more willing to engage in some of the risky behaviors, such as downloading apps from untrusted sources (Harris, Chin, & Brookshire, 2015), than females. The present study extends previous work and contributes to the research literature in two important ways: first, this study presents an updated evaluation of the current security practices of undergraduate business students using data collected through a survey administered in December 2019; second, we compare current results with those obtained in earlier studies (Jones & Chin, 2015; Jones & Heinrichs, 2012) and provide a comparative analysis of student behavior regarding smartphone security practices. This is an extremely important contribution because, while previous studies clearly show that students are lax in their security practices, these have only been snapshots of behavior at one point in time. The current study uses the same survey instrument that was used in 2014 and also in 2011 (Jones & Heinrichs, 2012), at the same southeastern university in the USA, therefore, we are afforded an opportunity to examine behavioral trends.

METHODOLOGY

Survey Instrument

To determine changes in security practices over time, students in business classes at a comprehensive regional university were surveyed in the fall semesters of 2014 and 2019. A student population was chosen because this generation represents zealous adopters of smartphone technology (Fidan, 2019; Jones & Chin, 2015). The same questionnaire was used in each time period, with minor updates that did not affect the meaning of any of the questions (the substance of smartphone security from a user perspective has changed little over these years). The survey instrument was originally developed in 2011 (Jones & Heinrichs, 2012) after conducting a review of the previously published literature to determine which smartphone security practices were most often recommended. The survey instrument was used again for an updated assessment of security behaviors (Jones & Chin, 2015). The survey instrument is not a comprehensive collection of all possible mitigating techniques and behaviors, but rather those most generally agreed upon to be helpful in avoiding an information disaster. As in the previous studies (Jones & Chin, 2015; Jones & Heinrichs, 2012), the survey questions were categorized into three groupings, as those related to ‘avoiding harmful behaviors and activities,’ ‘providing protection through phone settings and add-on utilities,’ and ‘preparing for disaster recovery’ as shown in Table 1. The survey instrument included six demographic questions asking such things as age, gender, and included major and type of cell phone, the remaining questions addressed security/privacy matters. No pilot study was conducted as the questionnaire had been tested and implemented in multiple prior studies.

Table 1: *Identified Security Practices by Approach*

Approach	**Practice**
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 anti-malware • Apply remote services: remote lock, remote wipe • Disable GPS when not in use
Avoid harmful behaviors and activities	• Do not apply software updates • Click on links in text messages and emails • Download risky third-party applications • Connect to known networks
Prepare for disaster recovery	• Avoid phone loss • Immediately report phone loss • **Record IMEI number** • Back up data • Insure phone • Remote lock and/or remote wipe features

Data collection for the current study took place in December 2019 from a similar population of business students at the same public university as collected in spring 2014 by Jones and Chin (2015). The proliferation of smartphones has mushroomed during this time gap, and therefore, it is important to provide an updated assessment and analysis. The present study affords the opportunity to gauge current student attitudes and practices with mobile security devices and to provide an understanding of changes in behaviors over time, if any.

Research Questions & Hypotheses

As in Jones and Heinrichs (2012) and Jones and Chin (2015), the purpose of this research is to study the following research questions:

> ***RQ1:*** *To what degree do business students practice recommended smartphone security approaches?*
>
> ***RQ2:*** *In what ways have security practices of business students changed over time?*

In addition to presenting the results of the data collection from the December 2019 administration of the survey instrument, we extend the previous studies and evaluate the following three hypotheses as we compare and contrast our current results to those from our 2014 administration of the same survey instrument (Jones & Chin, 2015):

> ***H1:*** *Student behavior in "avoiding harmful behaviors and activities" has positively increased from 2014 to 2019.*
>
> ***H2:*** *Student behavior in "providing protection through phone settings and add-on utilities" has positively increased from 2014 to 2019.*
>
> ***H3:*** *Student behavior in "preparing for disaster recovery" has positively increased from 2014 to 2019.*

RESULTS AND DISCUSSION

Survey responses were analyzed using frequency analysis. Additionally, to examine the statistical significance of responses between 2014 and 2019, Pearson's Chi-Square (p<.05) was used. Standardized residuals (Chou & Wang, 2010) were examined to determine the strength of the significance.

The data in Table 2 below shows the breakdown of respondents' type of phone by year (n=527). Only those respondents with "Smartphone with data package" were used for analysis in this study because those who pay for a data package were likely to be frequent users of smartphone features. Our sample size, therefore, totaled 504 students who used a smartphone with a data package (n=197 in 2014 and 307 in 2019). Of this sample of 504 students, 321 (36%) were female and 183 (64%) were male; this ratio held steady for both years of the study.

Table 2: *Cell Phone Type (All Respondents)*

	2014		**2019**	
Smartphone with data package	197	(90.3%)	307	(99.4%)
Smartphone no data package	5	(2.3%)	2	(0.6%)
Regular cell phone	14	(6.4%)	0	(0.0%)
No cell phone	1	(0.5%)	0	(0.0%)
Not sure or Other	1	(0.5%)	0	(0.0%)
Total	218	(100.0%)	309	(100.0%)

As expected, because the survey was administered in business classes, most of the respondents were business majors (see Table 3 below).

Table 3**:** *Respondent Major (Smartphone Respondents Only)*

	2014		**2019**	
Business	181	(81.2%)	279	(90.9%)
Arts & Sciences	9	(4.6%)	2	(0.6%)
Education	1	(0.5%)	1	(0.3%)
Science & Technology	18	(9.1)	11	(3.6%)
Undeclared/Other	9	(4.6%)	14	(4.6%)
Total	218	(100.0%)	307	(100.0%)

Tables 4, 5 and 6 below present the frequency analyses of survey responses, organized by security approach.

Table 4 shows responses on questions relating to “avoiding harmful behaviors and activities,” Table 5 depicts user responses concerning “providing protection through phone settings and add-on utilities,” and Table 6 presents the data relating to “preparing for disaster recovery.”

Table 4: *Behaviors and Activities – Application Software*, 2014 (*italics*) and 2019 (**bold**)

Survey Question Pearson Chi-Square indicating significance of difference between years (2014 and 2019)	**Yes or Frequently**	**Maybe or Sometimes**	**No or Never**	**Don't Know**	***Total**
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? Pearson Chi-Square = .014	*50* *25%* **52** **17%**	*55* *28%* **69** **22%**	*86* *44%* **168** **55%**	*6* *3%* **18** **6%**	*197* *100%* **307** **100%**
2. Have you or would you click on a website link received in an email or text from an unknown source? Pearson Chi-Square = .001	*29* *15%* **23** **7%**	*47* *24%* **50** **16%**	*118* *60%* **220** **72%**	*3* *1%* **14** **5%**	*197* *100%* **307** **100%**
3. Have you or would you download apps from an Internet source that you are not totally positive you could trust? Pearson Chi-Square = NS	*31* *16%* **48** **15%**	*52* *27%* **64** **21%**	*104* *53%* **177** **58%**	*8* *4%* **18** **6%**	*195* *100%* **307** **100%**
4. Have you or would you download an app that requested access to your contacts or other personal information? Pearson Chi-Square = NS	*101* *52%* **139** **45%**	*38* *19%* **58** **19%**	*52* *27%* **87** **28%**	*4* *2%* **23** **8%**	*195* *100%* **307** **100%**
5. Do you use your phone for financial purposes such as buying things online, checking your bank balance, making payments, etc? Pearson Chi-Square = .000	*87* *44%* **194** **63%**	*84* *43%* **97** **31%**	*23* *12%* **14** **5%**	*3* *1%* **2** **1%**	*197* *100%* **307** **100%**
6. Do you check for updates to your phone at least monthly? Pearson Chi-Square = NS	*141* *72%* **202** **66%**	*N/A* **N/A**	*52* *27%* **101** **33%**	*2* *1%* **4** **1%**	*195* *100%* **307** **100%**

*Not all students answered all questions, so the total does not always equal 197 (2014).

Table 5: *Use of Phone Settings and Add-on Utilities, 2014 (italics) and 2019 (**bold**)*

Survey Question Pearson Chi-Square indicating significance of difference between years (2014 and 2019)	**Yes/Always Most of the time**	**Sometimes**	**No or Never**	**Feature not available**	***Don't know**	**Total**
1. Have you set the idle timeout (so that the screen goes dark) to a shorter time than the factory default? Pearson Chi-Square = .045	*104* *53%* **133** **43%**	*NA* **NA**	*86* *44%* **151** **49%**	*NA* **NA**	*7* *3%* **23** **8%**	*197* *100%* **307** **100%**
2. To wake up after idle, is a password or other code required on your smartphone? Pearson Chi-Square = .000	*119* *60%* **278** **90%**	*NA* **NA**	*77* *39%* **25** **8%**	*NA* **NA**	*1* *1%* **4** **2%**	*197* *100%* **307** **100%**
3. Do you disable Bluetooth when it's not in use? Pearson Chi-Square = .000	*125* *68%* **116** **37%**	*26* *14%* **95** **31%**	*28* *15%* **95** **31%**	*NA* **NA**	*5* *3%* **1** **1%**	*184* *100%* **307** **100%**
4. Do you disable GPS (navigation) when you are not using it? Pearson Chi-Square = .001	*108* *58%* **119** **39%**	*35* *18%* **78** **25%**	*37* *19%* **93** **31%**	*NA* **NA**	*9* *5%* **16** **5%**	*189* *100%* **306** **100%**
5. When you use your phone to connect to WI-FI wireless networks, do you only connect to encrypted, password-protected networks? Pearson Chi-Square = .000	*91* *48%* **204** **69%**	*72* *38%* **75** **24%**	*14* *7%* **9** **3%**	*NA* **NA**	*14* *7%* **19** **6%**	*191* *100%* **307** **100%**
	Frequently	**Sometimes**	**Rarely /Never**	**Not installed**	***Don't know**	**Total**
6. Select one answer regarding anti-virus software: "Anti-virus software has been downloaded and installed on my phone and I use it …" Pearson Chi-Square = NS	*38* *19%* **59** **19%**	*25* *12%* **48** **16%**	*50* *26%* **71** **23%**	*50* *26%* **61** **20%**	*34* *17%* **68** **22%**	*197* *100%* ***307*** ***100%***
7. Select one answer regarding encryption software: "Encryption software has been downloaded and installed on my phone and I use it…" Pearson Chi-Square = NS	*20* *10%* **42** **14%**	*16* *8%* **32** **10%**	*66* *34%* **83** **27%**	*36* *18%* **48** **16%**	*59* *30%* **102** **33%**	*197* *100%* **307** **100%**

*Includes both "I don't know if this feature is present" and "I don't know if I have done or do this" responses.

Table 6: *Disaster Preparedness, 2014 (italics) and 2019 (**bold**)*

Survey Question **Pearson Chi-Square indicating significance of difference between years (2014 and 2019)**	**Yes**	**No**	**Don't Know**	**Total**
1. Before reading this question, did you record your phone's International Mobile Equipment (IEME) number? Note: you would have called #60# to get the number. Pearson Chi-Square = .029	*7* *4%* **29** **10%**	*158* *80%* **222** **72%**	*32* *16%* **56** **18%**	*197* *100%* **307** **100%**
2. Do you have an insurance policy on the phone? Pearson Chi-Square = .001	*93* *47%* **111** **36%**	*88* *45%* **138** **45%**	*16* *8%* **58** **19%**	*197* *100%* **307** **100%**
3. 2014: If you have insurance, please indicate below which of the following features the insurance policy provides: [Remote wipe] 2019: Do you know if either you or your insurance company has the ability to remotely wipe your phone (if lost or stolen)? Pearson Chi-Square = .000	*46* *40%* **55** **18%**	*19* *16%* **35** **11%**	*51* *44%* **217** **71%**	*116* *100%* **307** **100%**
4. 2014: If you have insurance, please indicate below which of the following features the insurance policy provides: [Remote lock] 2019: Do you know if either you or your insurance company has the ability to remotely lock your phone (if lost or stolen)? Pearson Chi-Square = .005	*43* *38%* **76** **25%**	*20* *17%* **32** **10%**	*52* *45%* **199** **65%**	*115* *100%* **307** **100%**
5. Have you ever permanently lost a smartphone? Pearson Chi-Square = NS	*33* *17%* **59** **19%**	*162* *82%* **245** **80%**	*1* *1%* **3** **1%**	*196* *100%* **307** **100%**
6. Do you store any pin numbers and/or passwords in your phone? (e.g. bank account pin numbers typed in as contacts so you can look them up) Pearson Chi-Square = .000	*57* *29%* **192** **63%**	*137* *69%* **111** **36%**	*3* *2%* **4** **1%**	*197* *100%* **307** **100%**
7. Do you ever back up the list of contacts that is stored on your phone? Pearson Chi-Square =NS	*147* *75%* **245** **80%**	*36* *18%* **43** **14%**	*12* *7%* **19** **6%**	*195* *100%* **307** **100%**
8. If you ever disposed of a smartphone, did you (or someone else) remove any memory cards first and/or wipe it clean of personal data (e.g. contacts, texts, account numbers, etc.)? Pearson Chi-Square =NS	*90* *78%* **192** **81%**	*21* *18%* **28** **12%**	*5* *4%* **16** **7%**	*116** *100%* **236*** **100%**

*In 2014 seventy-seven (39%) had not disposed of a smartphone; in 2019 seventy-one (23%) had not disposed of one.

In the following sections, we discuss the results in each of the three categories shown in Tables 4, 5 and 6 above.

Avoiding harmful behaviors and activities

Of the many actions one may take to limit risk and increase security of one's smartphone, six are categorized by the authors as "behaviors and activities." Four of these are things that should not be done, one of these (updating operating system regularly) should be performed, and the last one of these (use your phone for financial purposes) should be executed only with caution.

In Table 4, #1-3, we list some of the most critical behaviors to avoid. These are (1) opening multimedia attachments received in a text or email from an unknown source, (2) clicking on a website link received in an email or text from an unknown source, and (3) downloading apps from an Internet source you are not totally positive you can trust. This is particularly important because malware can end up on phones where users engage in such behaviors (Computer Hope, 2020; page, n.d.).

Hypothesis 1 was supported in that response percentages on these three questions reveal decreases in dangerous behavior from 2014 to 2019. Two of these behaviors show a statistically significant difference: opening multimedia attachments (Pearson's Chi-Squared =.014) and clicking on website links from unknown sources (p=.001). Analysis of standardized residuals indicates there are large differences in the YES ("I have and definitely would") and the NO ("I have not and definitely would not") responses for opening attachments and in the YES ("I have and definitely would") and the MAYBE (I have not but I might) responses for clicking on website links. Later year (2019) responders are less likely to open or click on such links. There is no statistical difference, but on the question about downloading apps from untrusted sources, responses follow the same pattern with fewer responders admitting to acting unwisely. The fact that students use more care with these behaviors is a positive finding. The fact that 39% still do or would open a multimedia attachment from an unknown source, almost a fourth (23%) do or would open a link to a website from an unknown source, and over a third (36%) download apps from sources they are not sure they can trust, is still worrisome.

Another behavior users should be wary of is downloading apps that request access to personal information or phone features (as shown in Table 4, #4). According to an article published by CNET in September, 2019, the author noted that other than regular OS updates the major threat comes from apps that "demand" excessive permissions to access the data and then leak it (Hodge, 2020). While it makes sense for a location app such as Google Maps to ask permission to access your location information, for example, other apps should not ask for access to your location your contacts, phone, or camera. Even if it makes sense for an app to access personal data, there are dangers. One might want Facebook (FB) to have access to the camera in order to add photos to their timeline easily. However, November 2019 news reports describe a FB "glitch" in certain iOS devices that caused the camera to activate when FB was accessed and allowed for capture of the content on the screen and where the fingers were positioned (Schuman, 2019). The device would only allow this to happen if the users had given the Facebook app access to the camera. Privacy issues such as these have caused both Google and Apple concern. The newly released Android 10 and iOS 13 have new security features that give the user more control over how often apps can access their location. Previously, tracking Android app permissions was frustratingly difficult, but now it has a one-click reject button for each item in a condensed list.

In order to take advantage of such features, however, users need to be aware of this issue and be willing to take the steps necessary to prevent apps from accessing unnecessary personal data. Our survey results show the percentage of people unconcerned with sharing personal data with apps ("I have or definitely would" download such apps) dropped from 52% in 2014 to 45% in 2019 while the percent who 'didn't know' increased from 2% to 8%. The difference broached significance at p=.051 for use for financial purposes. The fact that fewer people in 2019 are willing to download apps that request personal data than in 2014 is a positive trend, however, the bottom line is that 64% of respondents may be, or definitely are willing to download such apps.

More people in 2019 are using their phone for financial purposes and are using it more often (p=.000). In 2019, only 5% of respondents "Never" used their phone for financial purposes, meaning they do not use their phone for paying bills, checking bank balances or transferring money or other transactions (down from 12% in 2014). Frequent users jumped from 44% in 2014 to 63% in 2019. This type of phone use means smartphone owners should be particularly security conscious. They should be taking the utmost care to minimize the chance that malware is introduced onto their phone, transmissions are compromised, or stolen phones are unprotected by a passcode.

Weaknesses in security and outright glitches are fixed through updates to Android and Apple devices. Users, therefore, should be vigilant about installing such updates when notified by software providers that a new version is available. Because updating the operating system is seen as the most important security behavior a user can perform (Hodge, 2020), it is a positive development that OS providers are moving towards automatically and seamlessly updating phones in the background (Hodge, 2020). In the meantime, users should update their software regularly. When surveyed "do you check for updates at least monthly," 72% responded "Yes" in 2014, down to 66% in 2019, though this difference was not statistically significant. This leaves a high percentage of users not performing this critical security step.

As an aside, it is possible users have some reluctance to allow changes to their current operating system because providers have indeed used updates to slow down the performance of older phones in order to spur sales of new phones (Ganti, 2018; Kelly, 2018). This behavior discourages users from installing updates and this is inexcusable given how important such updates are to privacy and security.

In summary, Hypothesis 1 is supported because smartphone users' behaviors have improved significantly. Users are less likely to open multimedia attachments received in a text or email from an unknown source, less likely to click on a website link received in an email or text from an unknown source, and (though not statistically significant) the pattern is the same when it comes to downloading apps from an Internet source that they are not totally positive they can trust and allowing apps to have access to personal data. The one change in this category that introduces more risk to users comes as no surprise, and that is significantly more users execute financial transactions on their phones. Overall, the positive trend in this category is gratifying to see. Nevertheless, as discussed above, while there has been improvement, there are still too many users not following safe practices.

Providing protection through phone settings and utilities

Seven questions were included in this category. The first five questions revealed significant

differences in student behaviors between 2014 and 2019. The last two questions, asking about encryption and anti-virus usage, showed no differences between the two years.

The first question in this category asked if users have set the idle timeout to a shorter time than the manufacturers default (commonly, 30 seconds). Idle timeout is the time the phone will wait before going to sleep. Once asleep, if the user has set the device so that a passcode or biometric authentication is required, waking up the phone will require entering this passcode or thumbprint or, the latest variant, a facial scan (Withers, 2018). To set a shorter idle timeout is considered safer as 30 seconds can allow an unauthorized user sufficient time to pick up and use an unattended phone. Our survey results show that fewer respondents are now setting the timeout to a shorter time. In 2014, 53% set it to a shorter time; 43% now do so (p=.045).

On the other hand, a great many more users are protecting their phone with passcode or biometric authentication (p=.000). The percentage of those responding "Yes" to "To wake up after idle, is a password or other code required on your smartphone" went up from 60% to 90% between 2014 and 2019. This is a great improvement, and an important one because phones are vulnerable to being misplaced (Prey, 2019) and, even with the lockout-when-stolen capabilities, phones are still attractive to thieves (Borba, 2018). Even though there has been improvement in 2019 from 2014, the number of students choosing not to passcode protect their phone in 2019 still leaves many student phones vulnerable if these are stolen or lost. Given that there are 19 million undergraduate college students in the United States today (quora, 2018), assuming our study is generalizable, with 8% not password protecting their phones, that's over 1.5 million college students' phones alone and likely millions more unprotected phones in the general public.

The percentage of people "Always" turning off Bluetooth when not using it dropped from 68% to just 37%. This is a serious security concern because minimizing Bluetooth usage minimizes exposure risk. As an example of such risk, an attack vector called BlueBorne was disclosed by Armis in 2017. Blueborne is a set of vulnerabilities that the attacker can use to take complete control of a device and the data stored on it. Newman (2017) noted that it affected connected devices running Android, Linux, Windows, and iOS versions before iOS 10. A year later, even after multiple security patches, over two billion devices worldwide remain exposed either because they have not been updated, or because they will not receive updates at all (Seri, 2018). Other attacks have been known to crash devices, block phones from receiving calls, drain the phone's battery, and eavesdrop on conversations that phone owners are having with the people around them (and not just on their phone calls) (webroot, n.d.). Yet the percentage of respondents who *never* turn off Bluetooth when they are not using it has more than doubled (up to 31% from 15% in 2014).

GPS location services is another phone capability that creates privacy concerns (Flynn & Klieber, 2015). Our survey question asked respondents if they turned off GPS when not using it. The access to location information should be disabled for all apps unless you are specifically using the service to get to your destination. As addressed in a New York Times article in December 2018 (Valentino-Devries, Jennifer Singer et al., 2018), your phone is basically a tracking device. The NY Times found that at least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news, weather or other information. The NY Times reviewed a database containing information gathered in 2017 by one company; it revealed people's detailed travels, accurate to within a few yards, in some cases updated more than 14,000 times per day. Several businesses claim to track up to 200 million mobile devices in the United States. Incidentally, even if one turns off location services, researchers at Princeton have proven it is still possible to use other phone data to determine a person's location (Zorabedian, 2015). These researchers stated that there is no evidence to suggest commercial apps are engaged in this kind of data collection and tracking, but there is no easy way to ascertain this because their software is proprietary. Nevertheless, turning off GPS is at least making an effort to maintain one's privacy. Apparently, many of our survey respondents do not feel concerned, as 31% never turn off their location services (2019), a rise from 19% in 2014. Only 39% always disable GPS in 2019; in 2014 this figure was 58%. This difference between the years is significant at p=.001.

Another phone utility allows users to access the Internet via Wi-Fi. Users should only join safe, encrypted, password-protected networks and avoid unsecured public Wi-Fi access. The biggest threat with unsafe Wi-Fi is the "man-in-the-middle" attack, where the hacker positions himself between the user and the connection point. Then, he can intercept anything the user sends, including emails, credit card information, ID's and passwords if the user logs into a secured site via the Wi-Fi. Another possibility is that hackers can distribute malware (Chin, Little, & Jones, 2020). In this area our respondents showed a significant (p=.000) improvement between 2014 and 2019 in their awareness and behavior. Only 3% of current respondents showed no concern on this issue, "never" connecting to unsecure networks (compared to 7% in 2014). Sixty-nine percent (69%) "always" connect to safe WiFi in 2019 compared to 48% in 2014 (p=.000).

When it comes to anti-virus software, smartphones are not designed like computers. iPhones use a "sandbox" design where apps are restricted to their area and cannot migrate, or infect, other areas of the phone. Thus, "viruses" are not able to infect the entire system and a true anti-virus does not exist (Hoffman, 2018).

In the case of Androids, there is a question as to the efficacy of any anti-virus software used. Instead, common sense and careful phone usage is recommended (Whitwam, 2020). Users who are careful to download apps from legitimate sources (App Market for iPhones and Google Play for android), do not open email attachments from unknown sources or do not visit sketchy websites, are less likely to have their phones infected. Even with the utmost care, however, infection can happen. In summer 2019, twenty-five million Androids were infected with an app that was downloaded from the legitimate Google Play store (Ferguson, 2019). When asked about anti-virus software usage, respondents were given the choices: Anti-virus software is installed on my phone and I use it (a) Frequently (b) Sometimes (c) Never or (d) Phone is not equipped with anti-virus software or (e) Don't know. Responses were spread out over the five answers fairly evenly, and that held true in both 2014 and 2019. When only iPhones user responses were analyzed, responses again were spread out evenly over the answers; the same was true for Android users. Either users are not savvy when it comes to anti-virus software, or iPhone users have purchased products claiming to be anti-virus (a simple Google search for "iPhone antivirus" brings up as many advertisements selling anti-virus software as it brings up articles saying why anti-viruses don't exist or aren't real anti-viruses). Most likely, students in general are simply not knowledgeable about the phone anti-virus issue.

A similar pattern was seen in the question on encryption, with percentages responding to the (a) to (e) choice being close to identical in both years, 2014 and 2019. Again, when 2014 responses were compared by phone type and 2019 were compared by phone type, responses followed the same pattern regardless of whether the phone used was an android or an iPhone. Since the 3GS came out in 2008, Apple has consistently built 256-bit AES encryption into iOS devices (Team, n.d.). Encryption is enacted when the user's passcode protects his/her phone. With the release of Marshmallow 6.0 in October 2017, Google began requiring all Android manufacturers to encrypt by default (Brown, 2017). Again, the encryption feature is turned on when the user sets a passcode. Given the number of respondents in both 2014 and 2019 who answered "Don't know," "Sometimes" (encryption is either on or off) and "Phone does not have this feature" (all did except some Androids prior to 2014), it is safe to say that users are generally unfamiliar with encryption on their smartphones.

In summary, Hypothesis 2 was not supported. There is significant improvement in students' use of a password/passcode/biometric authentication to wake up their phone after idle. Users also seem to be more cognizant of the dangers of unprotected, public Wi-Fi with many more users only signing on to public networks if they are secured by a password. Three other areas, however, show decreased security concerns. Users are less likely to turn off Bluetooth and disable GPS when not using these features and fewer users have set idle timeout to a shorter time than the default time. The most critical of these is the disabling of Bluetooth; the fact that those users "always" disabling it dropped from 68% to just 37% is worrisome.

Preparing for disaster recovery

The final category of user security measures deals with the disaster of losing a phone or having one stolen. In this section, we evaluate Hypothesis 3, that is, student behavior in "preparing for disaster recovery" has positively increased from 2014 to 2019.

If one knows their phone's identifying IMEI (international mobile equipment identity) number, they can notify their provider and have their phone locked if it is lost or stolen (Jones & Chin, 2015). Leiva-Gomez (2018) notes that when a carrier knows a device has been stolen, it can blacklist the IMEI code and lock it out of the network. Later on, it tells other cellular networks to do the same. On the survey question asking if they had recorded their IMEI number, there is a statistically significant improvement in behavior between 2014 and 2019 (p=.029). The improvement is insignificant in practical terms, however. While only 4% had recorded their IMEI number in 2014, a mere 10% had done so in 2019. And while in 2014, 80% had not recorded it, in 2019 this percentage was still high, at 72%. Those who did not know if they had recorded the IMEI number stayed about the same (16% in 2014 and 18% in 2019).

The percentage of students who answered 'Yes' to "Do you have insurance on your phone" decreased significantly (p=.001). The percentage dropped from 47% in 2014 to 36% in 2019, though that is not the whole picture. The percentage of people who responded "no" is exactly the same in both years at 45%. The change that offsets the decrease in "Yes" responses is the "I don't know" answer, which increased from 8% to 19%. So, it cannot be determined whether fewer respondents have insurance or whether more respondents just don't know whether or not they have insurance.

Similarly, a large number of respondents do not know if they have remote wipe capabilities on their phone, a feature that could be very helpful if their phone is lost or stolen. Responses for 2014/ 2019 were 40%/18% "Yes"; 16 %/11% "No" and 44%/71% "I don't know." The most noticeable change is the high percentage of students who are not aware of the remote wipe feature. Today's phones all have this feature and setting up your phone to be able to use it is not at all difficult (University Northern Michigan, n.d.). The same pattern of responses was seen in the question about remote lock. Responses for 2014/2019 were 38%/25% "Yes"; 20%/32% "No" and 45%/ 65% "I don't know." Again, people are not aware of these phone capabilities. Given that the 18-24 year old age group has their cell phones lost or stolen at a higher rate than any other age group in the general population (Statista Research Department, 2012), these phone resources are important security features that students should know.

In terms of lost or stolen phones, our survey respondents appear to be more fortunate than the general population of 17 to 24-year-olds. In our sample, only 19% of the 2019 respondents and 17% of the 2014 respondents (p=NS) had a phone go permanently missing, while it has been reported that 45% of that age group in the general population have had phones misplaced or misappropriated (Statista Research Department, 2012).

There are many types of private data stored on phones, including texts, photos, contacts, Whatsapp and FB messages. One particularly critical type of information that users may store on their smartphones is pin numbers or user credentials to log into work databases; banking, retirement or other financial institutions; and stores where the user makes purchases. A question on the survey asked if users stored pin numbers and/or passwords on their phone. There is a marked change in behavior over the time period of our study. Significantly more people are storing such information on their phones in 2019 than in 2014 (p=.000). While 29% of people in 2014 did so, 63% store this kind of information on their phone in 2019. The implication, not surprisingly, is that people use their phone for many more tasks now, and they place a great deal of trust in the device protecting the privacy of their stored information. If pin numbers and passwords fall into the wrong hands, this most likely creates problems for the phone owner. One mitigating factor, when it comes to a lost or stolen phone, is that very few people who store this kind of data on their device have neglected to password protect their phone. Specifically, in 2014, 77 out of 197 (39%) did not passcode protect their phone. Of these 77, only 16 respondents stored pin numbers and/or passwords on their phone. In 2019, only 24 out of 307 (8%) did not have a passcode on their phone, and of these 24, 12 responded that they stored pin numbers or passwords on their phone. So, in our overall sample, very few people stored this sensitive information on a phone unprotected by a passcode. This does not negate the issue of hackers, however, and as mentioned above, if people are downloading apps with malware or using unsafe WiFi, having this kind of information present on the phone presents a real danger.

In case of a lost phone, it would be helpful if the phone's content were backed up. Our survey question specifically asked if respondents had ever backed up their contact list ("Yes" answer includes those contact lists that are automatically synced by their email host, such as Gmail). There were no significant differences in the percentages between the two years. In 2014, 75% did back up contacts and 80% did so in 2019. There was also no change in behavior on the question of whether they wiped their phones before disposing of them. Most people do take this precaution: 78% in 2014 and 81% in 2019 wiped their phone before disposal.

In summary, Hypothesis 3 was not supported for the results do not reflect a positive improvement in student behavior in "preparing for disaster recovery" between 2014 and 2019. Although five of the survey questions showed statistically significant differences, the practical implications of four of these questions were negligible. Specifically, while the number of people who have recorded their IMEI number is statistically higher, only 10% of users have recorded it. The number of users whose phone is covered by insurance has decreased offset only by the number of "don't know" responses, and the majority of users do not know if their phone has remote lock or remote wipe features. The one question where the change is of practical significance, and is particularly concerning, is the increase in the number of users who store pin numbers and passwords on their phone. The number of users who do so increased from 29% in 2014 to 63% in 2019.

SUMMARY, CONCLUSIONS & FUTURE RESEARCH DIRECTIONS

This substantial usage and penetration of mobile devices, in particular smartphones, into mainstream daily life renders knowledge of and adherence to appropriate security measures and practices imperative. To help protect the rich assortment of sensitive data, Chin, McRae, Jones and Harris (Chin, McRae, et al., 2016) recommend that colleges and universities publish mobile security artifacts, where artifacts is defined as policies, procedures, guidelines or other documented or undocumented protocols that clearly address use, connectivity and access, of any and all mobile devices. Policies are mandatory practices that must be followed and guidelines are suggested practices that should garner adherence.

While technical measures can be instituted to help assuage some security concerns, educating users and managing their practices when using their devices is vital (Chin, Etudo, & Harris, 2016) as this is arguably the weakest link in security (Mylonas, Kastania, & Gritzalis, 2013; Zhang, Li, & Deng, 2017). Smartphone users' security - and privacy - related decisions are influenced by their attitudes, perceptions, and understanding of various security threats (Alsaleh, Alomar, & Alarifi, 2017).

In the current study, the first category discussed was “Avoiding harmful behaviors and activities.” Decreases in dangerous behaviors – opening multimedia attachments, clicking on website links, and downloading apps from untrusted sources – generally show improvement, in that fewer people responded that they engage in these activities. But this improvement does not completely mitigate the issue because over a third of the respondents indicated that they would or might open such multimedia attachments and almost a fourth stated they would or might click on such potentially harmful website links. When it comes to downloading apps from sources, they were not sure they could trust, in 2019 fewer answered that they do this “Frequently,” but this was simply offset by more people answering “Don’t Know” so this is not really an improvement. When it comes to downloading apps requesting access to personal information, there was no significant difference between 2014 and 2019. This behavior is still concerning as forty-five percent (45%) “Frequently” allow new apps access to personal data. The last item in this category deals with frequency of checking for updates. The percentage of those who check for updates at least monthly has not changed significantly over the five years between 2014 and 2019. Currently, one-third (33%) of respondents do not check for updates that frequently. Fortunately, a mitigating factor is the move towards automatic, seamless smartphone updates by smartphone providers. Overall, in the “Avoiding harmful behaviors and activities” category, there has been improvement in user behaviors over the past five years and also improvement in phone technology such as automatic updates. But improving from poor security awareness to not-quite-as-poor security does not solve the issue. In general, users cannot be trusted to take the precautions necessary to protect the integrity and security of the data on their phones.

Results on the second category, “Use of phone settings and add-on utilities,” were mixed. One conclusion drawn from student responses is that students are not fully aware of their phone’s encryption capabilities nor the phone’s need (or lack thereof) of anti-virus software. This was true for both 2014 and 2019 and for both Android and iPhone users. The other five survey items all showed significant differences between the years. In two cases, setting a passcode on the phone and being sure to use encrypted, password-protected Wi-Fi, there was improvement. It was encouraging to find 90% of the students passcode their phone. This could be partly due to the ease of using a thumbprint now. Also, 69% (as opposed to 48% in 2014) now “Always” use safe Wi-Fi. Conversely, fewer people set the idle timeout to longer than the factory default, fewer disable GPS when they aren’t using it, and fewer disable Bluetooth. Regarding the critical issue for security, that of disabling Bluetooth, 31% indicated that they never disable it. The mixed results in this category reveal once again that security measures are not used to the extent that they should be used in order to maintain integrity and security of students’ smartphones.

The final category concerned “Disaster preparedness.” Five of the seven survey questions in this category showed significant changes between 2014 and 2019. One improvement is that more people have recorded their phone’s IEME number. However, the percentage only increased from 4% to 10%. People need to know this number in order to report a lost or stolen phone to their providers. Fewer respondents appear to have insurance and fewer know whether their phone has remote lock or remote wipe. Further, a great deal more people store pin numbers and/or passwords on their phone (up from 29% to 63%). These results indicate that students are not prepared for the misfortune of losing their phone.

Our study has shown that while there is improvement in some areas of smartphone security behaviors, there is a worsening in other areas. Even in the improved areas, the improvement often does not mean current behavior can be considered “good;” it is simply better than it was. Smartphone security requires awareness and vigilance and, overall, based on the questionnaire responses, at the present time security-conscious behavior is simply not the norm.

From our study, it is clear that smartphone providers must continue to work on enhancing the security of their devices. Obviously, this is something that they have done since the inception of cell phones (see for example, (Long, 2016)). Our study also shows how vital it is that organizations use care when allowing their employees to use their personal phones as a BYOD (bring your own device) to connect their devices to the company network. Mobile devices present a variety of risks that need to be addressed. The company policies should include requirements such as “must password protect,” “device must lock itself with pin or passcode if it is idle for xx minutes,” “employees may only download apps that appear on the company’s list of approved apps,” “when using Wi-Fi to connect to the internet, only secure password-protected WiFi may be used,” “turn off Bluetooth when not using it” and so on. Hopefully, having employees attest to understanding such policies will raise employee awareness concerning these very important security issues.

Finally, it is clear that users need to be more aware of smartphone security measures. Future research in this area should address the question of how best to educate consumers, especially if they are using their phones as a BYOD. We recommend surveying employees from different types of businesses to see if those working for businesses requiring a higher level of privacy/security (such as those in the medical profession) have higher security awareness levels. If it is found that they do, one could research what educational practices were most effective. Given that our 2019 study unveiled so little improvement in user behavior over a five-year period, perhaps the most important research direction is to study possible security measures providers can add to enhance device security for their users. Regardless of the specific directions taken, additional research in smartphone security and consumer behavior is clearly needed in order to improve the state of affairs in this vital area.

REFERENCES

Alsaleh, M., Alomar, N., & Alarifi, A. (2017), "Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods". In *PLoS ONE* (vol. 12, no.3). https://doi.org/10.1371/journal.pone.0173284

Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. (2020), "Employees’ behavioural intention to smartphone security: A gender-based, cross-national study". *Computers in Human Behavior*, vol. 104(October 2019). https://doi.org/10.1016/j.chb.2019.106184

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021), "Keeping customers’ data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce". *Computers in Human Behavior*, vol. 114 (April 2020), 106531. https://doi.org/10.1016/j.chb.2020.106531

Amez, S., & Baert, S. (2020), "Smartphone use and academic performance: A literature review". *International Journal of Educational Research*, vol. 103 (April). https://doi.org/10.1016/j.ijer.2020.101618

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018), "Taxonomy of mobile users’ security awareness". *Computers and Security*, vol. 73, pp. 266–293. https://doi.org/10.1016/j.cose.2017.10.015

Borba, A. (2018), "*Despite Anti-Theft Features, Thieves Still Seek Out iPhones"*. CBS SF Bay Area. https://sanfrancisco.cbslocal.com/2018/01/30/despite-anti-theft-features-thieves-seek-out-iphones/

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020), "A survey on smartphone user’s security choices, awareness and education". *Computers and Security*, vol. 88. https://doi.org/10.1016/j.cose.2019.101647

Brown, M. (2017), "*Here’s how cell phone encryption works"*. Inverse. Retrieved from https://www.inverse.com/article/38639-cell-phone-encryption-how-it-works

Cate, F. H. (2006),. "The Privacy and Security Policy Vacuum in Higher Education". *Educause Review*, vol. 41, no. 5, p. 18.

Chaffey, D. (2020), *Mobile marketing statistics compilation*. Smart Insights. Retrieved from https://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

Chin, A. G., Etudo, U., Harris, M. A., Goyal Chin, A., Etudo, U., & Harris, M. A. (2016), "On mobile device security practices and training efficacy: An empirical study". *Informatics in Education*, vol. 15, no. 2, p. 235.

Chin, A. G., Harris, M., & Brookshire, R. (2021), "An Empirical Investigation of Intent to Adopt Mobile Payment Systems Using A Trust-Based Extended Valence Framework". *Information Systems Frontiers*.

Chin, A. G., Little, P., & Jones, B. (2020), "An Analysis of Smartphone Security Practices among Undergraduate Business Students at a Regional Public University Amita G Chin Philip Little". *International Journal of Education and Development Using Information and Communication Technology*, vol. 16, no. 1, pp. 44–61.

Chin, A. G., McRae, D., Jones, B. H., & Harris, M. A. (2016), "An Exploration of Mobile Device Security Artifacts At Institutions Of Higher Education". *Journal of International Technology and Information Management*, vol. 25, no. 3, pp. 27–52.

Chou, Y.-T., & Wang, W.-C. (2010), "Checking dimensionality in item response models with principal component analysis on standardized residuals". *Educational and Psychological Measurement*, vol. 70, no. 5, pp. 717–731.

Computer Hope. (2020), "*Can smartphones get infected with viruses or malware?"* Computer Hope. https://www.computerhope.com/issues/ch001818.htm

Current World Population. (2020). WorldOMeter. https://www.worldometers.info/world-population/

Damaševičius, R., Maskeliunas, R., Venčkauskas, A., & Woźniak, M. (2016), "Smartphone user identity verification using gait characteristics". *Symmetry*, vol. 8, no. 10. https://doi.org/10.3390/sym8100100

Das, A., & Khan, H. U. (2016), "Security behaviors of smartphone users". *Information and Computer Security*, vol. 24, no. 1, pp.116–134. https://doi.org/10.1108/ICS-04-2015-0018

Elrefaei, L. A., Hamid, D. H., Bayazed, A. A., Bushnak, S. S., & Maasher, S. Y. (2018)., "Developing Iris Recognition System for Smartphone Security". *Multimedia Tools and Applications*, vol. 77, no. 12, 14579–14603. https://doi.org/10.1007/s11042-017-5049-3

Farshidfar, N., & Hamedani, S. (2020), "The Potential Role of Smartphone-Based Microfluidic Systems for Rapid Detection of COVID-19 Using Saliva Specimen". *Molecular Diagnosis and Therapy*, vol. 24, no. 4, pp. 371–373. https://doi.org/10.1007/s40291-020-00477-4

Felisoni, D. D., & Godoi, A. S. (2018), "Cell phone usage and academic performance: An experiment". *Computers and Education*, vol. *117*(October 2017), pp.175–187. https://doi.org/10.1016/j.compedu.2017.10.006

Ferguson, C. (2019), "*Malicious apps infect 25 million Android devices with "Agent Smith" malware"*. Phys.Org. https://phys.org/news/2019-07-malicious-apps-infect-million-android.html

Fidan, M. (2019), "Development of a scale for university students' Facebook use purposes and an examination in terms of their Facebook use profiles". In *International Journal of Education and Development using Information and Communication Technology (IJEDICT,* vol. 15, no. 4, pp.132-150.

Flynn, L., & Klieber, W. (2015), "Smartphone Security". *IEEE Pervasive Computing*, vol. 14, no. 4, pp.16–21. https://doi.org/10.1109/MPRV.2015.67

Furnell, S., & Phippen, A. (2012), "Online privacy: A matter of policy?" *Computer Fraud and Security*, *2012* vol. 8, pp.12–18. https://doi.org/10.1016/S1361-3723(12)70083-0

Ganesh, A., Sahu, P., Nair, S., & Chand, P. (2020), "A smartphone based e-Consult in addiction medicine: An initiative in COVID lockdown". *Asian Journal of Psychiatry*, vol. 51(April), 102120. https://doi.org/10.1016/j.ajp.2020.102120

Ganti, A. (2018), "*Samsung Lied About Not Using Updates to Slow Down Older Phones"*. Wccftech. https://wccftech.com/samsung-lied-about-not-using-updates-to-slow-down-older-phones/

Gikas, J., & Grant, M. M. (2013), "Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones & social media". *Internet and Higher Education*, vol. 19, pp.18–26. https://doi.org/10.1016/j.iheduc.2013.06.002

Gunuc, S., & Kuzu, A. (2015), "Confirmation of Campus-Class-Technology Model in student engagement: A path analysis". *Computers in Human Behavior*, vol. 48, pp.114–125. https://doi.org/10.1016/j.chb.2015.01.041

Harris, M. A., Brookshire, R., & Chin, A. G. (2016), "Identifying factors influencing consumers' intent to install mobile applications". *International Journal of Information Management*, vol. 36, no. 3, pp. 441–450. https://doi.org/10.1016/j.ijinfomgt.2016.02.004

Harris, M. A., & Chin, A. G. (2016), "Consumer trust in Google's top developers' apps: An exploratory study". *Information and Computer Security*, vol. 24, no. 5, pp. 474–495. https://doi.org/10.1108/ICS-11-2015-0044

Harris, M. A., Chin, A. G., & Beasley, J. (2019), "Mobile Payment Adoption: An Empirical Review and Opportunities for Future Research". *Southern Association of Information Systems (SAIS)*, *March*, 7.

Harris, M. A., Chin, A. G., & Brookshire, R. (2015), "Mobile app installation: the role of precautions and desensitization". *Journal of International Technology and Information Management*, vol. 24, no. 4, p. 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 and Security*, vol. 10, no. 4, pp. 186–202. https://doi.org/10.1080/15536548.2014.974429

Hart-Davis, G. (2010), "*iPad & iPhone Administrator's Guide: Enterprise Deployment Strategies and Security Solutions"*. McGraw-Hill Education Group.

He, J., & Freeman, L. A. (2010), "Are Men More Technology-Oriented Than Women? The Role of Gender on the Development of General Computer Self-Efficacy of College Students*"*. *Journal of Information Systems Education*, vol. 21, no. 2, pp. 203-212

Hodge, R. (2020), "*iOS 13 vs. Android 10: Which OS is more secure?"* Cnet. https://www.cnet.com/news/ios-13-vs-android-10-which-os-is-more-secure/

Hoffman, C. (2018), "*What's the Best Antivirus for iPhone? None!"* Howtogeek. https://www.howtogeek.com/352613/what's-the-best-antivirus-for-iphone-none/

Hydara, I., Sultan, A. B. M., Zulzalil, H., & Admodisastro, N. (2015), "Current state of research on cross-site scripting (XSS) - A systematic literature review". In *Information and Software Technology*, vol. 58, pp.170–186. Elsevier. https://doi.org/10.1016/j.infsof.2014.07.010

Johns, M. (2014), "Script-templates for the content security policy". *Journal of Information Security and Applications*, vol. 19, no. 3, pp. 209–223. https://doi.org/10.1016/j.jisa.2014.03.007

Jones, B. H., & Chin, A. G. (2015), "On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time". *International Journal of Information Management*, vol. 35, no. 5, pp. 561–571. https://doi.org/10.1016/j.ijinfomgt.2015.06.003

Jones, B. H., Chin, A. G., & Aiken, P. (2014), "Risky business: Students and smartphones". *TechTrends*, vol. 58, no. 6, pp. 73–83.

Jones, B. H., & Heinrichs, L. R. (2012), "Do business students practice smartphone security?" *Journal of Computer Information Systems,* vol. 53, no. 2, pp. 22-30

Kelly, H. (2018), "*What to do if you think Apple's slowing down your phone"*. CNN Business. https://money.cnn.com/2017/12/22/technology/apple-iphone-slowdown/index.html

Kim, E. B. (2014), "Recommendations for information security awareness training for college students". *Information Management and Computer Security*, vol. 22, no. 1, pp.115–126. https://doi.org/10.1108/IMCS-01-2013-0005

Kim, I., Kim, R., Kim, H., Kim, D., Han, K., Lee, P. H., Mark, G., & Lee, U. (2019), "Understanding smartphone usage in college classrooms: A long-term measurement study". *Computers and Education*, vol. 141 (March), 103611. https://doi.org/10.1016/j.compedu.2019.103611

Leiva-Gomez, M. (2018), *No Title*. Maketecheasier. https://www.maketecheasier.com/imei-number/

Liao, P. A., Chang, H. H., Wang, J. H., & Sun, L. C. (2016),. "What are the determinants of rural-urban digital inequality among schoolchildren in Taiwan?" Insights from Blinder-Oaxaca decomposition. *Computers and Education*, vol. 95, pp.123–133. https://doi.org/10.1016/j.compedu.2016.01.002

Long, J. (2016), "*The Evolution of iOS Security and Privacy Features"*. Intego. https://www.intego.com/mac-security-blog/the-evolution-of-ios-security-and-privacy-features/

Marett, K., Pearson, A. W., Pearson, R. A., & Bergiel, E. (2015), "Using mobile devices in a high risk context: The role of risk and trust in an exploratory study in Afghanistan". *Technology in Society*, vol. 41, pp. 54–64. https://doi.org/10.1016/j.techsoc.2014.11.002

Mensch, S., & Wilkie, L. (2011), "Information security activities of college students: an exploratory study". *Academy of Information and Management Sciences Journal*, vol. 14, no. 2, pp. 91-116

Mi, T., Gou, M., Zhou, G., Gan, Y., & Schwarzer, R. (2020), "Effects of planning and action control on smartphone security behavior". *Computers and Security*, vol. 97, 101954. https://doi.org/10.1016/j.cose.2020.101954

Minaie, A. (2011), "Integration of mobile devices into computer science and engineering curriculum". In Conference proceedings: 2011 ASEE Annual Conference & Exposition. DOI:10.18260/1-2--18267

Mobile Fact Sheet. (2019). Pew Research Center, Internet & Technology. https://www.pewresearch.org/internet/fact-sheet/mobile/

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015), "Measuring user satisfaction with information security practices". *Computers and Security*, vol. 48, pp. 267–280. https://doi.org/10.1016/j.cose.2014.10.015

Motiwalla, L. F. (2007), "Mobile learning: A framework and evaluation". *Computers and Education*, vol. 49, no. 3, pp. 581–596. https://doi.org/10.1016/j.compedu.2005.10.011

Mylonas, A., Kastania, A., & Gritzalis, D. (2013), "Delegate the smartphone user? Security awareness in smartphone platforms". *Computers and Security*, vol. 34, pp. 47–66. https://doi.org/10.1016/j.cose.2012.11.004

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

Nayak, J. K. (2018), "Relationship among smartphone usage, addiction, academic performance and the moderating role of gender: A study of higher education students in India". *Computers and Education*, vol. 123 (August 2017), pp. 164–173. https://doi.org/10.1016/j.compedu.2018.05.007

Newman, L. H. (2017),. "*Hey, Turn Bluetooth Off When You're Not Using It"*. Wired. https://www.wired.com/story/turn-off-bluetooth-security/

Nowrin, S., & Bawden, D. (2018), "Information security behaviour of smartphone users: An empirical study on the students of university of Dhaka, Bangladesh". *Information and Learning Science*, vol. 119, nos. 7-8, pp. 444–455. https://doi.org/10.1108/ILS-04-2018-0029

O'Dea, S. (2020), "*Forecast number of mobile devices worldwide from 2020 to 2024"*. Statista. https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/

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

Page, D. (n.d.), "*5 Ways Your Mobile Device Can Get Malware"*. SecurityMetrics. Retrieved October 10, 2020, from https://www.securitymetrics.com/blog/5-ways-your-mobile-device-can-get-malware

Palmer, D. (2019), "*Mobile malware attacks are booming in 2019: These are the most common threats"*. ZDNet. https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/

Park, J. H., Yi, K. J., & Jeong, Y. S. (2014), "An enhanced smartphone security model based on information security management system (ISMS)". *Electronic Commerce Research*, vol. 14, no. 3, pp. 321–348. https://doi.org/10.1007/s10660-014-9146-3

Patten, K. P., & Harris, M. A. (2013), "*The Need to Address Mobile Device Security in the Higher Education IT Curriculum"*. No Source

Prey, I. (2019), "*Prey Mobile Theft & Loss Report Finds 69 Percent of Missing Devices" Worldwide Simply Misplaced*. GlobeNewswire. https://www.globenewswire.com/news-release/2019/03/05/1748091/0/en/Prey-Mobile-Theft-Loss-Report-Finds-69-Percent-of-Missing-Devices-Worldwide-Simply-Misplaced.html

quora. (2018), "*How many college students are there in the United States?"* Quora. https://www.quora.com/How-many-college-students-are-there-in-the-United-States

Robertson, D. J., Kramer, R. S. S., & Burton, A. M. (2015)., "Face averages enhance user recognition for smartphone security". *PLoS ONE*, vol. 10, no. 3, pp. 1–11. https://doi.org/10.1371/journal.pone.0119460

Sansom-Daly, U. M., & Bradford, N. (2020), "Grappling with the "human" problem hiding behind the technology: Telehealth during and beyond COVID-19". *Psycho-Oncology*, vol. 29, no. 9, pp. 1404–1408. https://doi.org/10.1002/pon.5462

Schuman, E. (2019), "*Facebook's iOS "bug" secretly filmed users. IT, take note".* Computerworld. https://www.computerworld.com/article/3454619/facebooks-ios-bug-secretly-filmed-users-it-take-note.html

Seri, B. (2018), "*BlueBorne: One Year Later"*. Armis. https://www.armis.com/resources/iot-security-blog/blueborne-one-year-later/

Shah, P., & Agarwal, A. (2020), "Cybersecurity behaviour of smartphone users in India: an empirical analysis". *Information and Computer Security*, vol. 28, no. 2, pp. 293–318. https://doi.org/10.1108/ICS-04-2019-0041

Shropshire, J., Warkentin, M., & Sharma, S. (2015), "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior". *Computers and Security*, vol. 49, pp.177–191. https://doi.org/10.1016/j.cose.2015.01.002

Siponen, M., Pahnila, S., & Mahmood, A. (2006), "Factors influencing protection motivation and IS security policy compliance". *2006 Innovations in Information Technology*, pp.1–5.

Smith, A. (2011), "*Americans and Their Cell Phones"*. Pew Research Center, Internet & Technology. https://www.pewresearch.org/internet/2011/08/15/americans-and-their-cell-phones/

Statista Research Department. (2012). *No Title*. Statista. https://www.statista.com/statistics/241365/us-cell-phone-users-whose-device-has-been-lost-or-stolen-by-age-group/

Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2021), "Behavioral biometrics & continuous user authentication on mobile devices: A survey". *Information Fusion*, vol. 66 (July 2020), pp. 76–99. https://doi.org/10.1016/j.inffus.2020.08.021

Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Alsalem, M. A., Albahri, A. S., Alamoodi, A. H., Kiah, M. L. M., Jumaah, F. M., & Alaa, M. (2019), "Comprehensive review and analysis of anti-malware apps for smartphones". In *Telecommunication Systems* vol. 72, no. 2. Springer US. https://doi.org/10.1007/s11235-019-00575-7

Team, E. (n.d.), "*Why Default iPhone Encryption Isn't Enough"*. Virtru. Retrieved October 10, 2020, from https://www.virtru.com/blog/iphone-encryption/

Terzis, V., & Economides, A. A. (2011), "Computer based assessment: Gender differences in perceptions and acceptance". *Computers in Human Behavior*, vol. 27, no. 6, pp.2108–2122. https://doi.org/10.1016/j.chb.2011.06.005

University Northern Michigan. (n.d.), "*Setting up remote wipe on your mobile device"*. Northern Michigan University. Retrieved October 10, 2020, from https://it.nmu.edu/docs/setting-remote-wipe-your-mobile-device

Valentino-Devries, Jennifer Singer, N., Keller, M. H., & Krolik, A. (2018), "*Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret"*. NewYork Times. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

Verkijika, S. F. (2018), Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret". *Computers and Security*, vol. 77, pp.860–870. https://doi.org/10.1016/j.cose.2018.03.008

webroot. (n.d.), "*A Review of Bluetooth Attacks and How to Secure Your Mobile Device"*. Webroot. Retrieved October 10, 2020, from https://www.webroot.com/au/en/resources/tips-articles/a-review-of-bluetooth-attacks-and-how-to-secure-mobile-workforce-devices

Whitwam, R. (2020), "*Android Antivirus Apps Are Useless — Here's What to Do Instead"*. Extremetech. https://www.extremetech.com/computing/104827-android-antivirus-apps-are-useless-heres-what-to-do-instead

Withers, R. (2018), "*The iPhone's Face ID Struggles in the Morning"*. Slate. https://slate.com/technology/2018/07/iphone-face-id-struggles-to-recognize-people-in-the-morning.html

Wong, K., Wang, F. L., Ng, K. K., & Kwan, R. (2015), "*Investigating Acceptance towards Mobile Learning in Higher Education Students BT - Technology in Education". Transforming Educational Practices with Technology* (K. C. Li, T.-L. Wong, S. K. S. Cheung, J. Lam, & K. K. Ng (Eds.); pp. 9–19). Springer Berlin Heidelberg.

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012), "The effect of online privacy policy on consumer privacy concern and trust". *Computers in Human Behavior*, vol. 28, no. 3, pp. 889–897. https://doi.org/10.1016/j.chb.2011.12.008

Yazdanmehr, A., Wang, J., & Yang, Z. (2020), "Peers matter: The moderating role of social influence on information security policy compliance". *Information Systems Journal*, vol. 30, no. 5, pp. 791–844. https://doi.org/10.1111/isj.12271

Yoon, H. S., & Occeña, L. (2014), "Impacts of customers' perceptions on internet banking use with a smart phone". *Journal of Computer Information Systems*, vol. 54, no. 3, pp.1–9. http://www.scopus.com/inward/record.url?eid=2-s2.0-84900863413&partnerID=40&md5=89040d2b805f11d80a0e0e12096933d6

Zeldin, A. L., Britner, S. L., & Pajares, F. (2008), "A comparative study of the self-efficacy beliefs of successful men and women in mathematics, science, and technology careers". *Journal of Research in Science Teaching*, vol. 45, no. 9, pp.1036–1058. https://doi.org/10.1002/tea.20195

Zhang, X. J., Li, Z., & Deng, H. (2017), "Information security behaviors of smartphone users in China: An empirical analysis". *Electronic Library*, vol. 35, no. 6, pp. 1177–1190. https://doi.org/10.1108/EL-09-2016-0183

Zhao, Y., Ni, Q., & Zhou, R. (2018), "What factors influence the mobile health service adoption? A meta-analysis and the moderating role of age". *International Journal of Information Management*, vol. 43 (May 2017), pp. 342–350. https://doi.org/10.1016/j.ijinfomgt.2017.08.006

Zhou, G., Gou, M., Gan, Y., & Schwarzer, R. (2020), "Risk Awareness, Self-Efficacy, and Social Support Predict Secure Smartphone Usage". *Frontiers in Psychology*, *11*(June), 1–8. https://doi.org/10.3389/fpsyg.2020.01066

Zorabedian, J. (2015), "*T-Mobile customers hit by Experian breach get credit monitoring by Experian"*. Nakedsecurity by Sophos. https://nakedsecurity.sophos.com/2015/10/02/t-mobile-customers-hit-by-experian-breach-get-credit-monitoring-by-experian/