*International Journal of Education and Development using Information and Communication Technology (IJEDICT),* 2020, Vol. 16, Issue 1, pp. 44-61

# An Analysis of Smartphone Security Practices among Undergraduate Business Students at a Regional Public University

**Amita G Chin**
**Virginia Commonwealth University, USA**

**Philip Little**
**Coastal Carolina University, USA**

**Beth H Jones**
**Western Carolina University, USA**

## ABSTRACT

In 2019, the number of smartphone users in the United States was estimated to be over 266 million, or 81% of the population. While smartphones, combined with a plethora of apps that are readily available, have become wholly integrated into our daily lives, they embody a multitude of risks for consumers. The purpose of this study is to assess smartphone security practices among undergraduate business students at a regional public university. In December 2019, a survey focusing on security-related practices was administered to students in multiple business classes at the university. The results of the survey show that students exhibit a high degree of care on some measures of security, but they are rather lax in other areas. Males exhibit evidence of some more risky behaviors than their female counterparts. Those who have lost their phones in the past are more likely to be familiar with some disaster preparedness phone features and they are more likely to insure their smartphones.

**Keywords:** *Smartphone security, business students, mobile devices, cell phones*

## INTRODUCTION

Over the past decade, mobile device usage has grown at a phenomenal rate. In late 2016, the use of mobile technologies surpassed desktop usage when visiting websites (Heisler, 2016). In 2018, 58% of site visits were from mobile devices (Enge, 2019). In fact, over 50 percent of all website traffic worldwide is being generated through mobile phones (Clement, 2019).

This growth in mobile technologies is having an enormous impact on businesses. TrendMicro surveyed 600 companies in five countries, each employing at least 500 employees (TrendMicro, 2012). The results revealed that 56% of the companies surveyed allowed employees to use their own mobile device for work-related activities (75% of United States respondents allowed such employee use). This phenomenon exposes companies to considerable risk. Verizon commissioned an independent research company to survey more than 600 professionals involved in managing mobile devices for their organizations (Verizon, 2019) and reported that 33% of the organizations admitted to having suffered a compromise that involved a mobile device - up from 27% in their 2018 report. Sixty-two percent of those affected described the compromise as major while 41% also described it as major but added that this was with lasting repercussions. Sixty-seven percent of organizations said they are less confident about the security of their mobile assets than other devices, yet only 45% had mobile endpoint security in place. Nearly half of the companies, 48%, admitted to sacrificing security to "get the job done."

Universities and colleges are among the most aggressive adopters of wireless technology as collaboration and open learning is fueled by the presence of mobile devices (Jones & Heinrich, 2012). Students want to incorporate mobile phones into the classroom learning experience, including using apps, listening to podcasts and accessing learning systems (Dolawattha, Jayewardenepura, & Lanka, 2019; Chin, Etudo & Harris, 2016). In a 2017 survey of 520 students, approximately 94% responded that they wanted to use their smartphones in class for academic purposes (Kelly, 2017).

In 2019, the number of smartphone users in the United States was estimated to be over 266 million (O'Dea, 2020), or 81% of the population. While smartphones, combined with the plethora of apps that are readily available, have become wholly integrated into our daily lives, they embody a multitude of risks for businesses and consumers. For example, most consumers use their smartphone as a repository of vast personal data, including address information, contacts, appointments, bank information, and passwords. While biometric security precautions such as faceID may thwart some unauthorized access, a host of additional security infractions may occur, resulting in an unsanctioned exposure of personal data. Clearly, mobile device security has become a significant issue.

## LITERATURE REVIEW

The convenience of mobile technology has provided the impetus for a ubiquitous saturation, however, such widespread usage presents significant implications for consumer safety (Wang, Streff, & Sonell, 2012; Zonouoz, Houmansadr, Berthier, Borisov, & Sanders, 2013; Zhao, Zhang, Ge, & Yuan, 2012; van Cleeff, 2008;). As with desktop computers and laptops, mobile devices are susceptible to hacking and other malicious infringements. Malware compromises, for example, can occur in the form of viruses, worms, Trojan horses (Gohring, 2006), and spyware. A smartphone that has been victimized could volunteer owner data, financial data, personal information for all of the owner's contacts, banking information and passwords, email, texts, photos, and video. Such malware attacks can have devastating repercussions for consumers and for organizations (Liang & Xue, 2010), especially if the smartphone is used as a BYOD (bring your own device). However, instituting security measures on a personal device is a matter of consumer choice, and ignorance and apathy often dominate decision making. Even though many significant malware attacks (Wang et al., 2012; Felt et al., 2011) have been reported, most users remain unaware of preventive measures (Paullet & Pinchot, 2014).

Previous research literature focusing on the security practices of college students when using their smartphones signals that students are remiss in their behavior (Kim, 2014). For example, users routinely download software from unknown or questionable websites onto their mobile devices, creating potential security breaches for malware and other infractions (Mylonas et al., 2013a, 2013b; Zonouoz et al., 2013; Jones, Chin, & Aiken, 2014; Zhao et al., 2012). In addition to unsafe downloads, college students are particularly prone to leaving their cell phone on a desk in their classroom or on a table during a social event. Theft of mobile devices is common, where AP (2012) notes that more than 40 percent of all robberies now involve cell phones. Gupta et al., (2014) indicate that theft of these devices has become the fastest growing undetectable crime. Apart from the financial distress of losing a smartphone, the loss of contact information, passwords, calendars, and other data can cause particular setbacks, anxiety, and other emotional distress in the daily lives of the device owners (Gupta et al., 2014).

To more accurately gauge the smartphone security practices of college students and to determine the potency of these practices, several researchers have administered survey instruments and analyzed the collected data (Terzis & Economides, 2011; Padilla-Meléndez, Aguila-Obra, & Garrido-Moreno, 2013), including an evaluation of trust and risk as antecedents to mobile app

installation (Chin et al., 2018). Mylonas et al. (2013a, 2013b) 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. Harris et al. (2015, 2016) confirmed that a certain desensitization exists amongst consumers. Jones & Chin (2015) compared attitudes between 2011 and 2014 and found a disturbing increase in the number of students that would open a multimedia attachment received in a text or email from an unknown source. Mensch and Wilkie (2011) compared security practices of college students and reported a "troubling disconnect" among information security attitudes, behaviors, and tool usage. Kim (2014) implemented a survey instrument to gauge the security awareness of college students and concluded that additional security awareness training is needed. 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.

The present study is a continuation of the work of Jones & Chin (2015) and Jones et al., (2014). In the former work, survey results collected from 205 undergraduate business students at a regional public university were analyzed. The study found that students were lax in their mobile security practices, with men more willing to engage in some of the risky behaviors than women. The present study extends previous work and contributes to the research literature in that this study presents an updated evaluation of the current security practices of undergraduate business students.

## METHODOLOGY

The purpose of this study is to assess smartphone security practices. The specific research question examined in this study is: What is the current state of smartphone security awareness and practices among college business students? Based on a literature review of security practices relating to smartphones conducted by Jones & Chin (2015), a survey was created and administered to students in eleven undergraduate business classes at a regional comprehensive university (two principles of management sections, one sports management class, one auditing class, five principles of accounting sections and two finance classes). A student population was chosen because this generation represents zealous adopters of smartphone technology (Jones & Chin, 2015; Fidan, 2019). College campuses face a challenging dilemma. Smartphones clearly have a powerful and significant presence on campus and are used not just for social interaction, but also increasingly so for access to academic material, submission of work, online research, and for financial transactions. This substantial usage and penetration into mainstream daily life makes knowledge of and adherence to appropriate security measures and practices imperative (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. These methods have been categorized into three groupings, as shown in Table 1 (Jones & Heinrichs, 2012). The survey was administered to over three hundred business students to determine their awareness of and behaviors related to smartphone usage. Survey responses were analyzed using frequency analysis and Pearson's Chi-Square ($p<.05$) as has been done previously by researchers in this area (Koyuncu & Pusatli, 2019). Standardized residuals were examined to determine the strength of the significance (Chou & Wang, 2010).

**Table 1:** *Identified Security Practices by Approach*

| Approach | Practice |
|---|---|
| Provide protection through phone settings and add-on utilities | ⁾ Enable encryption<br>⁾ Enable password protection<br>⁾ Enable lock/timeout for inactivity<br>⁾ Disable Bluetooth when not in use<br>⁾ Install anti-malware<br>⁾ Apply remote services: remote lock, remote wipe<br>⁾ Disable GPS when not in use |
| Avoid harmful behaviors and activities | ⁾ Do not apply software updates<br>⁾ Click on links in text messages and emails<br>⁾ Download risky third-party applications<br>⁾ Connect to known networks |
| Prepare for disaster recovery | ⁾ Avoid phone loss<br>⁾ Immediately report phone loss<br>⁾ **Record IMEI number**<br>⁾ Back up data<br>⁾ Insure phone<br>⁾ Remote lock and/or remote wipe features |

## Hypotheses

Researchers have studied the influence of gender on several aspects of technology (Elhai et al., 2017). The consensus is that males are generally more comfortable with computer technology than females. Referring to this phenomenon as "The Digital Divide," Cooper (2006) reviewed 20 years of related literature and concluded that women were at a disadvantage due to the presence of "computer anxiety." He further stated that this anxiety in turn leads to differences in attitudes and performance. Durndell & Haag (2002) and Schumacher & Morahan-Martin (2001) also found computer anxiety was more likely to be present in females. A more recent study (He & Freeman, 2010) concluded that females felt less confident with computers because they had learned less and practiced less, perhaps due to the low number of females that participate in STEM education. While these studies refer to computers in general and not mobile devices in particular, they could relate to the usage of the more technical aspects of smartphones. Specifically, females could feel less confident about the more technical aspects of their smartphones, such as anti-virus, encryption, setting timeouts and other phone settings and add-on utilities. Previous research also lends support to this notion as it concludes that females were less likely to use encryption on their smartphones and less likely to use only encrypted WiFi when using public WiFi (Jones & Heinrichs, 2012). Therefore, we posit the following hypotheses related to phone settings and add-on utilities:

*H1: Females are less likely to use phone setting and add-on utility phone capabilities than males*.

Security behaviors relating to application software includes activities such as using email and Facebook, texting, downloading apps and making online purchases (Harris, Chin & Beasley, 2019). These applications normally require less technical acuity and have become more commonplace in everyday life than the built-in utilities discussed earlier, so one would not expect gender differences in their general use. However, there may be a gender difference when it comes to their safe use. Eckel & Grossman (2008) reviewed dozens of studies comparing risk behaviors of males and

females in many different contexts. These studies ranged from investment choices, abstract gambling experiments and the perceived risk associated with various recreational and social activities to the likelihood of engaging in such activities as illicit drug use and criminal activities. After the review of the literature, their conclusion was, "The findings from field studies conclude that women are more risk averse than men" (Eckel & Grossman, 2008, p. 12). In fact, several previous researchers have studied the differences in risk aversion between genders (Lam, 2014; Hibbert et al., 2013; Sapienza et al., 2009), concluding that women are more likely to avoid risky situations. Therefore, we hypothesize:

*H2: Females will demonstrate less risky behavior than males in security practices related to application software usage*.

Smartphones have evolved into being an essential component of life and well-being, such that most consumers maintain an emotional attachment to their device (Choi et al., 2012; Kim, 2013). Previous research (Hoffner, Lee & Park, 2016; Montag & Walla, 2016) has shown that phones contribute to a greater sense of "well-being" and that consumers exhibit "negative feelings, such as loneliness/disconnection, anxiety, and boredom" when separated from their mobile device (Hoffner, Lee & Park, 2016, p. 2452), often experiencing the five stages of grief of the Kübler-Ross model (Burnett, 2014). As portable mechanical devices, smartphones are expensive objects that are easy to misplace, lose, and damage. As with other valuable items such as homes, cars, computers, and PDAs, insurance is available for the damage, loss, or theft of a smartphone. While many users may not initially consider purchasing insurance for their smartphone, we hypothesize that:

*H3: Those who have lost a phone will be more likely to exhibit behaviors and awareness of smartphone features related to disaster preparedness.*

## RESULTS

In this study a total of 309 students responded to the survey. All of the respondents surveyed owned a smartphone. Two of these reported having smartphones with no data package (necessitating WiFi access to reach the internet); the rest all had smartphones with a data package. Eighty-four percent (84%) of the students who participated in this study used smartphones with an iOS operating system (iPhones); the other 16% were Android users.

In this study, 198 (64.1%) of the respondents were male and 111 (35.9%) were female. The breakdown by major is shown in Table 2, and as expected, since the surveys were administered in business classes, most students (91%) were business majors.

***Table 2:*** *Demographics: Gender and Major*

| Gender | | | | Total |
|---|---|---|---|---|
| | | Male | Female | |
| Major | Business | 182 | 98 | 280 (91%) |
| | Arts and Sciences | 0 | 2 | 2 (1%) |
| | Construction Management and Technology | 9 | 1 | 10 (3%) |
| | Education | 0 | 1 | 1 (0%) |
| | Health and Human Sciences | 4 | 7 | 11 (3%) |
| | Other | 3 | 2 | 5 (2%) |
| Total | | 198 | 111 | 309 (100%) |

### Use of Phone Settings and Add-on Utilities

Table 3 presents the results of a frequency analysis of the seven survey questions chosen to determine the degree to which the respondents use phone settings and add-on utilities. The results of the frequency analysis show that in one of the most critical areas, password protecting their phone, a high percentage of the respondents are engaging in security conscious behavior. Almost ninety-two percent (91.9%) of users' phones require a password to wake up after idle (92.3% of iPhone users and 89.8% of Android users require passwords). This is a particularly important feature; first, because it prevents unauthorized people from accessing data from a lost or stolen phone, and second, because iPhones automatically encrypt files when password protection is enabled. Android phones will perform in the same manner if the user has turned on encryption. It is also notable that 43% of the participants actually shortened the automatic timeout (that is, how much time before an idle phone sleeps) to a shorter time than the factory preset.

***Table 3*:** *Frequency Analysis of the Use of Phone Settings and Add-On Utilities*

| Survey Question | Y | S | N | FNA | *Don't know | Total | Gender | Have you lost a phone |
|---|---|---|---|---|---|---|---|---|
| 1. Have you set the idle timeout (so that the screen goes dark) to a shorter time than the factory default? | 133<br>43% | NA | 153<br>50% | NA | 23<br>7% | 309<br>100% | NS* | NS |
| 2. To wake up after idle, is a password or other code required on your smartphone? | 278<br>90% | NA | 25<br>8% | NA | 6<br>2% | 309<br>100% | NS | NS |
| 3. Do you disable Bluetooth when it's not in use? | 117<br>37% | 95<br>31% | 95<br>31% | NA | 2<br>1% | 309<br>100% | NS | NS |
| 4. When you use your phone to connect to WI-FI wireless networks, do you only connect to encrypted, password-protected networks? | 202<br>67% | 74<br>24% | 8<br>3% | NA | 18<br>6% | 302**<br>100% | NS | NS |
| 5. Do you disable GPS (navigation) when you are not using it? | 120<br>39% | 78<br>25% | 94<br>31% | NA | 16<br>5% | 308**<br>100% | NS | NS |
| 6. Select one answer regarding anti-virus software: "Anti-virus software has been downloaded and installed on my phone and I use it …" | 59<br>19% | 49<br>16% | 72<br>23% | 61<br>20% | 68<br>22% | 309<br>100% | --- | --- |
| 7. Select one answer regarding encryption software: "Encryption software has been downloaded and installed on my phone and I use it…" | 42<br>14% | 33<br>11% | 84<br>27% | 48<br>15% | 102<br>33% | 309<br>100% | --- | --- |

*Column title key: "Y" = Yes/Always/Most of the time; "S" = Sometimes; "N" = No/Never for questions 1-5 and Rarely/Never for questions 6 and 7; "FNA" = Feature not available/not installed*

* "NS" = Not significant. (Using Pearson's Chi-Square test, no statistically significant differences on this question between males/females or between those who have/have not lost a phone.)
**Users were instructed to leave related question blank if they did not use GPS, Bluetooth, or Wi-Fi. Seven respondents never used Wi-Fi; one respondent never used GPS. These were omitted from the relevant analysis.
*** Can include cases of both "I don't if this feature is present" as well as "I don't know if I have done or do this."

Another very important security protection is disabling bluetooth when it is not in use. If this feature is not disabled, it is easy for hackers to copy data from a smartphone when they are in close proximity. Of course, if the phone has password protection enabled, its encryption will help mitigate this problem. However, a non-password protected iPhone or an Android phone with encryption not turned on could have its unencrypted, sensitive data compromised. Interestingly, phone users may be aware of this because while only 33% of the iPhone users disable bluetooth "Always/Most of the time" (and over a third, 35%, "Never" disable bluetooth), Android users are more careful. Sixty-five percent (65%) of Android users disable bluetooth when not in use "Always/Most of the time" while only 12% of them "Never" disable it.

Another behavior very important in keeping a smartphone secure is to connect only to safe WiFi networks. It is well known that data sent through unguarded public networks can be intercepted from laptops and tablets, and this is true of smartphones as well. Given the type of sensitive data that can be accessed by a phone (for example, bank accounts, credit card accounts, and paypal) and personal data that may be sent, one should only connect via legitimate, encrypted, password-protected WiFi or via the phone's mobile network. Sixty-seven percent (67%) of respondents "Always/Most of the time" engage in safe WiFi practices. Twenty-four percent (24%) "Sometimes" engage and only 3% admit to "Never" worrying about safe WiFi sites.

Disabling GPS is more of a privacy issue than a possible data loss or compromised phone issue. Well over a third of the respondents (37%) disable GPS "Always/Most of the time"; 25% "Sometimes" disable it and 31% "Never" disable it.

Unlike computers and tablets, installing anti-virus software on smartphones is not quite as critical because attacks are not as common. In the case of iPhones, a true anti-virus doesn't even exist because the operating system is built for security. On iPhones, apps are restricted to their area and cannot migrate, or infect, other areas of the phone. In the case of Androids, the benefit of antivirus software is arguable. On one hand, it is questionable whether the cost of a "resource- and battery-hogging antivirus app on your phone that is going to plague you with irritating notifications" is worth the benefit when the risk of viral software is low (Black, 2019). If apps are downloaded only from legitimate sources (App Market for iPhones and Google Play for android), email attachments are not opened and sketchy websites are not visited, it is less likely that a phone will become infected. However, infection can happen (Harris, Chin & Brookshire, 2015). In summer 2019, twenty-five million Androids were infected with an app that was downloaded from the legitimate Google Play store.

As shown in Table 4, respondents were fairly evenly distributed across possible answers, and differences between Android and iOS users were not statistically significant.

***Table 4:*** *Comparison of iPhone and Android users:* ***"****Antivirus is on my phone and I use it…"*

| | Always-Frequently | Sometimes | Rarely - Never | Phone not equipped | Don't know | Total |
|---|---|---|---|---|---|---|
| Count (iPhone users) | 45 | 39 | 60 | 55 | 61 | 260 |
| % within OS | 17.3% | 15.0% | 23.1% | 21.2% | 23.5% | 100.0% |
| Standardized Residual | -.7 | -.3 | -.1 | .5 | .5 | |
| Count (Android users) | 14 | 10 | 12 | 6 | 7 | 49 |
| % within OS | 28.6% | 20.4% | 24.5% | 12.2% | 14.3% | 100.0% |
| Standardized Residual | 1.5 | .8 | .2 | -1.2 | -1.2 | |
| Count (all phones) | 59 | 49 | 72 | 61 | 68 | 309 |
| % within OS | 19.1% | 15.9% | 23.3% | 19.7% | 22.0% | 100.0% |

The pattern of responses regarding encryption was almost identical between users of the two phone types, with the average response being 14% "Always", 11% "Sometimes", 27% "Rarely/Never", 15% "Phone is not equipped with encryption" and 33% "Don't know." These response patterns provide evidence that users are not knowledgeable about encryption. Even though all phones have encryption capability, 20% of respondents said their phone did not have encryption. iOS, for example, uses encryption on its phone by default when a password to wake from idle is used. Since 92% of respondents woke their iPhones up with a password, 92% of Apple respondents should have answered "Always" or "Don't know" but responses were 14% and 33%, respectively. Google phones may or may not come from the manufacturer with encryption turned on by default. Either way, users can turn it on or off in the settings and if enabled this way, all user files are encrypted. Newer, more sophisticated Android phones give users control at the individual files level – letting them encrypt just certain files. It was for this reason users were given the "always, sometimes, never" choices on the questionnaire. The fact that response percentages were almost identical on each response, regardless of operating system leads us to question the veracity of all responses on this question. Students in general do not seem to understand whether it is on their phone, whether they use it, perhaps even what it is. This may be why iPhone already has and Google is heading towards setting encryption as the default setting on all new phones.

In summary, the security behavior is strong in some of the more important areas and weaker in others. The most important security control is to use a password/passcode or biometric (thumb print, voice recognition) protection on a phone. Ninety-two percent of respondents claim to protect themselves in this manner. Fifty percent have even set the time to wake up after idle to a shorter time than the manufacturer's default. Only one-third disable their bluetooth, however, leaving them vulnerable to hacking by bluetooth pairing. Two-thirds connect to WiFi only through encrypted, password-protected networks, which means one-third are vulnerable to having electronically sent data stolen. A little over a third do not disconnect GPS. As discussed above, respondents do not seem to be well-versed in anti-virus or encryption technologies on their phones.

### Avoid Harmful Behaviors and Activities

Table 5 presents the results of a frequency analysis of the seven survey questions chosen to determine the degree to which the respondents engage in security conscious behavior when using their smartphones. Each question offered four response choices: Yes or Always, Maybe or Sometimes, No or Never, and Don't Know. In Questions #1 and #7, a no answer indicates a lesser security awareness level than a yes answer. In Questions #2-#6, a no answer indicates a greater security awareness level than a yes answer.

**Table 5:** *Frequency Analysis of Behaviors and Activities – Application Software*

| Survey Question | Y | M | N | Don't Know | Total | Gender | Have you lost a phone |
|---|---|---|---|---|---|---|---|
| 1. Do you disconnect/log off email and social networking applications such as Facebook when you are done using them? | 24<br>8% | 58<br>19% | 220<br>72% | 2<br>1% | 304*<br>100% | NS** | NS |
| 2. Have you or would you open a multimedia attachment (e.g., pictures, video, audio) received in a text or email from an unknown source? | 53<br>17% | 69<br>22% | 168<br>55% | 19<br>6% | 309<br>100% | **p=.011** | **p=.002** |
| 3. Have you or would you click on a website link received in an email or text from an unknown source? | 24<br>8% | 50<br>16% | 221<br>72% | 14<br>4% | 309<br>100% | **p=.089** | **p=.014** |
| 4. Do you use your phone for financial purposes such as buying things online, checking your bank balance, making payments, etc? | 196<br>63% | 97<br>31% | 14<br>5% | 2<br>1% | 309<br>100% | NS | NS |
| 5. Have you or would you download apps from an Internet source that you are not totally positive you could trust? | 49<br>16% | 64<br>21% | 178<br>57% | 18<br>6% | 309<br>100% | NS | NS |
| 6. Have you or would you download an app that requested access to your contacts or other personal information? | 139<br>45% | 59<br>19% | 88<br>29% | 23<br>7% | 309<br>100% | NS | NS |
| 7. Do you check for updates to your phone at least monthly? | 203<br>66% | N/A | 102<br>33% | 4<br>1% | 309<br>100% | NS | NS |

*Column title key: "Y" = Yes/Always; "M" = Maybe/Sometimes; "N" = No/Never*

*This question also included the choice "I never use these applications." Five respondents never used it and are omitted from this item's analysis.

** "NS" = Not significant. (Using Pearson's Chi-Square test, no statistically significant differences on this question between males/females or between those who have/have not lost a phone.)

The results of the frequency analysis of Questions #1 and #7 reveal that a high percentage (72%) of the respondents are not engaging in security conscious behavior with respect to logging off email and social networking applications. However, two-thirds (66%) of the respondents do check for updates on their phones at least monthly thus enhancing the security of their phones.

The results of the frequency analysis of Questions #2-#6 reveal a similar dichotomy of security awareness of the respondents with respect to different aspects of harmful behavior and activities. Question #3 shows that a high percentage of users exhibit security awareness behavior: 72% "Never" click on a website link received in a text or email from an unknown source (8% would, 16% might). Question #2 shows 55% "Never" open multimedia attachments received in a text or email from an unknown source, while 17% would and 22% might, and Question #5 shows 57% "Never" download apps from an unknown Internet source while 16% would and 22% responded they might. These responses show some degree of sophistication because clicking links, downloading apps, and opening attachments are three of the main ways malware can be introduced onto a phone (Page, 2019).

Responses from Question #6 concerning downloading apps that request access to contacts or other personal information reveal that only 29% answered "No or Never." This is more of a privacy issue than a security issue, and here users may be faced with a trade off because many apps cannot be downloaded unless you agree to share contacts or location or other personal data (Harris, Brookshire & Chin, 2016; Harris & Chin, 2016). The low "no" response rate on this question is not unexpected.

The responses from Question #4 asking if the respondents used their phone for financial purposes indicate 94% of the respondents either always or sometimes use their phone for financial purposes thus making their phones highly vulnerable to the most sensitive information of all, their money. Hackers have designed mobile software that specifically targets financial information in order to steal money. One example of such software is *Exobot,* an extremely sophisticated android software was made widely available in 2018 when its source code was shared online (Bradley, 2019). With malware like this lurking, those who perform financial transactions with their phone (almost everyone in this study) should be particularly vigilant regarding malware prevention. While many respondents reported using care, almost one-fourth would or might click on a website link from an unknown source, and close to half would or might open a multimedia attachment in a text or email from an unknown source and would or might download apps from a questionable source (Chin, Harris, & Brookshire, 2018).

In summary, with respect to harmful behaviors and activities involving application hardware, improvement in security practices is clearly warranted. Only in the areas of updating phones (Question #6) and clicking on website links from an unknown source (Question #3) are a high majority of the respondents reporting a high degree of care. The responses of all the other questions indicate a low to moderate percentage of respondents engaging in good security practices. The relatively low level of security behaviors overall is particularly troubling given that 94% of the respondents indicate that they use their phones for financial purposes.

**Prepare for Disaster Recovery**

Table 6 presents the results of a frequency analysis of the seven survey questions chosen to determine the extent to which respondents prepare for a disaster. Each of the survey questions offered three response choices: Yes, No, and Don't Know. For all but one of the questions (Question #5) a "Yes" response indicates a higher security awareness but for Question #5, which

enquires about the storing of pin numbers or passwords, a "No" response indicates a higher security awareness.

***Table 6:*** *Frequency Analysis of Disaster Preparedness*

| Survey Question | Yes | No | Don't know | Total | Gender | Have you lost a phone |
|---|---|---|---|---|---|---|
| 1. Before reading this question, did you record your phone's International Mobile Equipment (IEME) number? | 30<br>10% | 222<br>72% | 57<br>18% | 309<br>100% | NS* | NS |
| 2. Do you have an insurance policy on the phone? | 113<br>36% | 138<br>45% | 58<br>19% | 309<br>100% | NS | **p=.008** |
| 3. Do you or does your insurance company have the ability to remotely wipe your phone (if it's lost or stolen)? | 55<br>18% | 33<br>11% | 221<br>71% | 309<br>100% | **p=.002** | **p=.063** |
| 4. Do you or does your insurance company have the ability to remotely wipe your phone (if it's lost or stolen)? | 77<br>125% | 31<br>10% | 201<br>65% | 309<br>100% | **p=.004** | **p=.020** |
| 5. 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) | 194<br>63% | 111<br>36% | 4<br>1% | 309<br>100% | NS | NS |
| 6. Do you ever back up the list of contacts that is stored on your phone? | 246**<br>80% | 44<br>14% | 19<br>6% | 309<br>100% | NS | NS |
| 7. 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, etc.?) | 192<br>81% | 29<br>12% | 17<br>7% | 238***<br>100% | NS | NS |

* "NS" = Not significant. (Using Pearson's Chi-Square test, no statistically significant differences on this question between males/females or between those who have/have not lost a phone.)
** "Yes" answers included those with contact lists in sync with email and therefore always backed up. Three respondents checked "contacts are not on my phone; stored on network provider" and were added to the "always" response.
***71 students had not disposed of a smartphone.

The answers given by the respondents for Questions #1-#4 reveal a disturbingly low level of security awareness with respect to disaster preparedness. Only 10% of the respondents had recorded their phone's IEME number. Every phone has a unique IEME number that can be used

to identify its make, model, and serial number. This is important information in case of theft. Just over a third (36%) have phone insurance, and 70% and 65% do not know about the remote wipe and remote lock feature, respectively. Sixty-three percent (63%) of the respondents store pin numbers and passwords in their phones. While all of these responses show a lack of disaster preparedness, the answers given by the respondents in Questions #6 and #7 do show that 80% back up contact lists and 81% removed memory cards or wiped the phone clean of personal data before disposing of a phone. Importantly, as previously discussed, 90% of the respondents password protect their phone, which is one of the most important safety precautions to take.

In summary, with respect to disaster preparedness, the responses mostly indicate a low to moderate level of security awareness.

**Results of Hypotheses Testing**

Overall, our study has pointed out several weaknesses in the behavior and attitudes of smartphone users. In the following section we examine if gender plays a role in behavior and whether those who have lost a cell phone (20%) are more security conscious than those who have not.

**Categorical Analysis**

In addition to the descriptive measures reported above, categorical analysis (Chi-Square) was done on two variables in the study: *gender* and whether a person had *lost a cell phone* or not. Because of the inexplicable responses on anti-virus and encryption, these two features were excluded from further analysis. Results show on some behaviors there are clear distinctions between males and females and between those who have lost a phone and those who have not.

*Gender*

In H1, we hypothesized that females would be less likely to use phone settings and add-on utilities. Survey results show no differences were found on questions concerning use of password, setting the idle timeout, disabling bluetooth and GPS, and connecting only to secure WiFi.

In H2, we hypothesized that females will demonstrate less risky behavior than males in security practices related to application software usage. Our survey results indicated gender differences in (1) opening a multimedia attachment (pictures, video, audio) received in a text or email from an unknown source ($p=.011$) and (2) clicking on a website link received in an email or text from an unknown source ($p=.014$). Further analysis of the standardized residuals showed the biggest difference was in the “I haven’t and definitely would not” cells. Females were much more likely not to open/click such attachments and links than their male counterparts.

Regarding disaster preparedness, males were more aware of the remote wipe ($p=.002$) and remote lock ($p=.004$) features than females. Eighty-eight percent (88%) of females answered “Don’t know” while 61% of males did not know whether their phone had a remote wipe feature. Similarly, 82% of females and 55% of males were unfamiliar with whether their phone could be remotely locked. This is consistent with males being more familiar with technical features of smartphones.

*Lost a Phone*

In H3, we hypothesized that those who have lost a phone will be more likely to exhibit behaviors and awareness of smartphone features related to disaster preparedness. However, our survey found no differences in the use of phone settings and add-on utilities between users who had and had not lost a phone (Table 3). Concerning application software behaviors and attitudes (Table 5), those people who had lost a cell phone were more likely to click on potentially dangerous

attachments and links (Questions #2 and #3, respectively), while those who had not lost a phone were less likely to click on such attachments and links. The reverse was also true; those who had not lost a cell phone were less likely to engage in such clicking. This appears to indicate a general carelessness, that is, those who click with little thought are also the ones who have more of a tendency to lose their phones and vice versa. It is unlikely this result is due to a gender difference because there were no differences in the percent of females and males who had phones lost or stolen (p=.189).

As expected, there was a significant difference between those who had lost a phone and those who had not on the question "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?" (p=.000). Those who had suffered a lost or stolen phone were much less likely to have wiped data/removed memory cards than those who had not. Those who had lost a phone were also significantly more likely to have purchased insurance (p=.008). They were also more likely to be aware of the remote wipe (p=.002) and remote lock (p=.004) features. It is logical that those who have lost a phone would be more aware of these features and would now be more likely to have purchased insurance for their phone.

## CONCLUSION

With the vast proliferation of smartphones across all aspects of society, security of these devices and protection of the data that resides on them has become paramount. Given that 100% of those surveyed owned a personal smartphone, this study clearly establishes the universal penetration and use of these devices amongst business undergraduates at a public institution of higher education (Chin, Jones & Harris, 2016). While some students do exhibit awareness and caution on some measures of security, many students are unaware, lax, or just apathetic in several other areas of security. As established in the extant literature, females continue to practice more risk averse behavior than their male peers, however, even females are careless with device security. While insurance from loss or damage is available, most consumers do not purchase this insurance. Those who have lost their phones in the past are more likely to be familiar with some disaster preparedness phone features and they are more likely to insure their devices.

The findings of this study yield several critical implications for information systems research in other settings such as work place organizations. The widespread penetration of mobile technology brings to the forefront security concerns for personal devices, and for the security of devices that are used to access organizational data (Harris & Patten, 2014; Ogren, 2008), especially since the line between personal and work devices has been blurred. The ready availability of personal devices, which are often used as BYOD, often leads to increased employee productivity, albeit at the sacrifice of security. Our survey results show that security precautions are not adopted comprehensively or consistently, and partial adoption leading to a false sense of confidence does not yield efficacy, leaving users more vulnerable than ever.

## LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

As with all research endeavors, this study has certain limitations. One main limitation in this research is that the survey was administered only to undergraduate students, and even that, only to business students. While the feedback from this population helps us to understand attitudes and behaviors toward smartphone usage, our results are not generalizable to the population as a whole. One future research direction is to include a far more diverse population in the survey administration. For example, undergraduate as well as graduate students could be included in the pool. Including a variety of majors in addition to business students could also yield interesting results. Sampling a non-student population, for example, people working in the IT and other industries, would help establish more widespread attitudes and behaviors. Another limitation of this

study is that our survey instrument only measures student perceptions of their behavior rather than their actual behavior. In a future study, observations of actual behavior could prove valuable. As with previous research (Chin, Etudo & Harris, 2016), our results clearly indicate that students, and possibly the general population as a whole, could benefit from education on mobile device security. A future research study that samples a population, then provides mobile security training, and then resamples the population to assess modification in attitudes and behaviors, if any, could provide invaluable insights.

## REFERENCES

AP. (2012). Thefts of cell phones rise rapidly nationwide. Retrieved January 24, 2020, from https://www.usatoday.com/story/tech/2012/10/20/thefts-of-cell-phones-rise-rapidly-nationwide/1646767/

Black, M. (2019). Do you need antivirus on Android? Retrieved January 24, 2020, from https://www.techadvisor.co.uk/how-to/google-android/antivirus-android-3668607/

Bradley, B. (2019). Watch out for this nasty malware that can steal your banking information. Retrieved January 24, 2020, from https://www.komando.com/security-privacy/exobot-banking-trojan-malware/564426/

Burnett, D. (2014). Losing your smartphone: five stages of grief. Retrieved January 24, 2020, from https://www.theguardian.com/science/brain-flapping/2014/dec/22/phone-smartphone-loss-damage-grief

Chin, A. G., Etudo, U., & Harris, M. A. (2016). On Mobile Device Security Practices and Training Efficacy: An Empirical Study. *Informatics in Education*, vol 15, no 2, pp. 235-252. https://doi.org/10.15388/infedu.2016.12

Chin, A. G., Harris, M. A., & Brookshire, R. (2018). A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *International Journal of Information Management*, vol 39, (May 2017), pp. 49–59. https://doi.org/10.1016/j.ijinfomgt.2017.11.010

Chin, A. G., Jones, B., & Harris, M. A. (2016). An Exploration of Mobile Device Security Artifacts at Institutions of Higher Education, vol 25.

Choi, H.-S., Lee, H.-K., & Ha, J.-C. (2012). The influence of smartphone addiction on mental health, campus life and personal relations - Focusing on K university students. *Journal of the Korean Data and Information Science Society*, vol 23, no 5, pp.1005–1015. https://doi.org/10.7465/jkdi.2012.23.5.1005

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. https://doi.org/10.1177/0013164410379322

Clement, J. (2019). Percentage of all global web pages served to mobile phones from 2009 to 2018. Retrieved January 24, 2020, from https://www.statista.com/statistics/241462/global-mobile-phone-website-traffic-share/

Cooper, J. (2006). The digital divide: The special case of gender. *Journal of Computer Assisted Learning*, vol 22, no 5, pp. 320-334. https://doi.org/10.1111/j.1365-2729.2006.00185.x

Dolawattha, D. D. M., Jayewardenepura, S., & Lanka, S. (2019). The Impact Model: Teachers' Mobile Learning Adoption in Higher Education H. K. Salinda Pramadasa Sabaragamuwa University of Sri Lanka, Sri Lanka Prasad M. Jayaweera. *International Journal of Education and Development Using Information and Communication Technology*, vol 15, no 4, pp. 71-88.

Durndell, A., & Haag, Z. (2002). Computer self-efficacy, computer anxiety, attitudes towards the Internet and reported experience with the Internet, by gender, in an East European sample. *Computers in Human Behavior*, vol 18, no 5, pp. 521--535. https://doi.org/10.1016/S0747-5632(02)00006-7

Eckel, C. C., & Grossman, P. J. (2008). Men, women and risk aversion: Experimental evidence. In C. Plott & V. Smith (Eds.), *Handbook of experimental economics results,* vol. 1, pp. 1061-1072). New York, NY. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract id=1883693

Elhai, J. D., Chai, S., Amialchuk, A., & Hall, B. J. (2017). Cross-cultural and gender associations with anxiety about electronic data hacking. *Computers in Human Behavior*, vol 70, pp.161-167. https://doi.org/10.1016/j.chb.2017.01.002

Enge, E. (2019). Where is the Mobile vs. Desktop story going? Retrieved January 24, 2020, from https://www.perficientdigital.com/insights/our-research/mobile-vs-desktop-usage-study

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,* pp. 3-13.

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

Gohring, N. (2006). New Trojan horses threaten cell phones. Retrieved January 24, 2020, from https://www.computerworld.com/article/2560827/new-trojan-horses-threaten-cell-phones.html

Gupta, K., Kumar, R., & Loothra, S. (2014). Smartphone security and contact synchronization. *Proceedings - 2014 4th International Conference on Communication Systems and Network Technologies, CSNT 2014*, pp. 621-625. https://doi.org/10.1109/CSNT.2014.130

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

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.

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., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, vol 22, no 1, pp. 97-114. https://doi.org/10.1108/IMCS-03-2013-0019

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.

Heisler, Y. (2016). Mobile internet usage surpasses desktop usage for the first time in history. Retrieved January 24, 2020, from https://bgr.com/2016/11/02/internet-usage-desktop-vs-mobile/

Hibbert, A. M., Lawrence, E. R., & Prakash, A. J. (2013). Does knowledge of finance mitigate the gender difference in financial risk-aversion? *Global Finance Journal*, vol 24, no 2, pp.140-152. https://doi.org/10.1016/j.gfj.2013.07.002

Hoffner, C. A., Lee, S., & Park, S. J. (2016). "I miss my mobile phone!": Self-expansion via mobile phone and responses to phone loss. *New Media and Society*, vol 18, no 11, pp. 2452-2468. https://doi.org/10.1177/1461444815592665

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. *Tech Trends*, vol 58, no 6, pp. 73-83. https://doi.org/10.1007/s11528-014-0806-x

Jones, B. H., & Heinrichs, L. R. (2012). Do Business Students Practice Smartphone Security? *Journal of Computer Information Systems*, *Winter*, pp. 22-30.

Kelly, R. (2017). Survey: 94% of Students Want to Use Their Cell Phones in Class. Retrieved from https://campustechnology.com/articles/2017/12/12/students-want-to-use-their-cell-phones-in-class.aspx

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, H. (2013). Exercise rehabilitation for smartphone addiction. *Journal of Exercise Rehabilitation*, vol 9, no 6, pp. 500-505. https://doi.org/10.12965/jer.130080

Koyuncu, M., & Pusatli, T. (2019). Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mobile Information Systems*, *2019*. https://doi.org/10.1155/2019/2786913

Lam, D. (2014). Gender differences in risk aversion among Chinese university students. *Journal of Gambling Studies*, vol 31, no 4, pp.1405-415. https://doi.org/10.1007/s10899-014-9492-z

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly: Management Information Systems*, vol 33, no 1, pp. 71-90. https://doi.org/10.2307/20650279

Mensch, S., & Wilkie, L. (2011). Information Security Activities of College Students: An Exploratory Study. *Journal of Management Information and Decision Sciences*, vol 14, no 2, p. 91.

Montag, C., & Walla, P. (2016). Carpe diem instead of losing your social mind: Beyond digital addiction and why we all suffer from digital overuse. *Cogent Psychology*, vol 3, no 1, pp.1-9. https://doi.org/10.1080/23311908.2016.1157281

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 and Security*, vol 38, pp. 51-75. https://doi.org/10.1016/j.cose.2013.03.007

O'Dea, S. (2020). Number of smartphone users in the United States from 2010 to 2023 (in millions). Retrieved March 28, 2020, from https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/

Ogren, E. (2008). Getting enterprises ready for smartphone security. Retrieved January 24, 2020, from http://blogs.computerworld.com/getting enterprises ready for smartphone security

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. Retrieved January 20, 2020, from https://www.securitymetrics.com/blog/5-ways-your-mobile-device-can-get-malware

Paullet, K., & Pinchot, J. (2014). Mobile malware: coming to a smartphone near you? *Issues in Information Systems*, vol 15, no 2, pp. 116-123. Retrieved from http://iacis.org/iis/2014/98_iis_2014_116-123.pdf

Sapienza, P., Zingales, L., & Maestripieri, D. (2009). Gender differences in financial risk aversion and career choices are affected by testosterone. *Proceedings of the National Academy of Sciences of the United States of America*, vol 106, no 36, pp. 15268-15273. https://doi.org/10.1073/pnas.0907352106

Schumacher, P., & Morahan-Martin, J. (2001). Gender, Internet and computer attitudes and experiences. *Computers in Human Behavior*, vol 17, no 1, pp.95-110. https://doi.org/10.1016/S0747-5632(00)00032-7

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

Trend Micro. (2012). Consumerization Survey Report The Consumerization of IT. Retrieved March 28, 2020, from https://www.trendmicro.de/cloud-content/us/pdfs/rpt_consumerization-survey-report.pdf

van Cleeff, A. (2008). Future consumer mobile phone security: A case study using the data-centric security model. *Information Security Technical Report*, vol 13, no 3, pp.112-117. https://doi.org/10.1016/j.istr.2008.10.003

Verizon. (2019). Mobile Security Index 2019 Executive Summary. Retrieved from https://enterprise.verizon.com/resources/reports/mobile-security-index/

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone Security Challenges. *Computer*, vol 45, no 12, pp. 52-58. https://doi.org/10.1109/MC.2012.288

Zhao, M., Zhang, T., Ge, F., & Yuan, Z. (2012). Robotdroid: A lightweight malware detection framework on smartphones. *Journal of Networks*, vol 7, no 4, pp. 715-722. https://doi.org/10.4304/jnw.7.4.715-722

Zonouz, S., Houmansadra, A., Berthiera, R., Borisova, N., & Sanders, W. (2013). Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. *Computers and Security*, vol 37, pp. 215-227. https://doi.org/10.1016/j.cose.2013.02.002