https://doi.org/10.48009/2_iis_2014_116-123
Issues in Information Systems
Volume 15, Issue II, pp. 116-123, 2014

MOBILE MALWARE: COMING TO A SMARTPHONE NEAR YOU?

Karen Paullet, Robert Morris University, paullet@rmu.edu
Jamie Pinchot, Robert Morris University, pinchot@rmu.edu

ABSTRACT

This study explored awareness and concern about mobile malware as well as usage habits related to preventative measures used to mitigate mobile malware risk factors. Several mobile malware risk factors were explored, including connecting to unsecured Wi-Fi networks, setting mobile devices to automatically connect to Wi-Fi networks, leaving Bluetooth connectivity on, reading reviews before downloading mobile apps, using anti-malware software or apps, frequency of data backups, and device locks using passwords, PINs, or fingerprints. A total of 187 participants were surveyed, including undergraduates and doctoral students and alumni at a mid-Atlantic university. The study found that among the risk factors explored, participants were not as aware of the dangers associated with connecting mobile devices to unsecured Wi-Fi networks and also were largely unfamiliar with anti-malware software and apps. A set of recommendations for increasing awareness of preventative security measures for mobile malware were also presented.

Keywords: mobile malware, mobile security, smartphone, Bluetooth, Wi-Fi

INTRODUCTION

Mobile phones have become ubiquitous within our society, and many would now consider them a necessity rather than a convenience. We are living in a world where people are staying connected via mobile technology more than ever before. Technology which was once only found on desktop computers can now be carried in the palm of our hands. The number of mobile phone users at the end of 2012 was approximately 5.9 billion worldwide [8]. Mobile devices allow people to have a constant connection to friends, family, and information. As we move about our day, one will notice people using their mobile devices almost everywhere. Users are staying connected while waiting in lines, at the bus stop, when dining out with family and friends, and in the car. This noticeable constant connection to our mobile devices is bringing to the forefront an area of concern in regard to security. What security mechanisms do we have in place to deal with mobile security threats? Most average computer users have some type of anti-virus or anti-malware software installed on their computers, but what about their mobile devices?

Malware is any computer program designed to infiltrate, use, or damage a device without the owner's consent. The term malware is often characterized as hostile, intrusive, malicious, or annoying [11]. In fact, the term itself is derived from "malicious software," and in common usage it has become an umbrella term to describe many different types of malicious computer programs. Mobile malware is any type of malware that is specifically targeted toward smartphones, tablets and other mobile devices. Mobile malware is on the rise and is projected to continue its upward trajectory, propelled by the large and continually growing smartphone user base and an increasingly mobile work force which provide enticing targets for hackers [12]. Leavitt [12] describes this phenomenon succinctly, "In the world of computers and communications, the more widely a technology is used, the more likely it is to become the target of hackers" (p. 11). The main goals of most mobile malware include theft of private information, incurring charges to premium numbers, or gaining access to a user's bank accounts or credit [5, 11, 15]. Mobile malware poses a serious threat and is evolving into a complex landscape that will likely soon rival that of traditional computer malware [5]. The number of security breaches to personal devices is difficult to measure, and few studies have explored this area to date. Our research seeks to explore awareness, concern and habits regarding numerous mobile device security issues.

RELATED LITERATURE

In order to be able to address the risk factors associated with mobile malware, it is imperative to first understand the threats [7]. The increased usage of mobile devices has introduced new security risks [20]. Mobile devices are becoming a new target to gain user information, as mobile device security has not kept up with traditional computer security. Cyber criminals are beginning to attack mobile devices due to the lack of security measures in place. Attacking mobile devices has become extremely attractive to criminals due to the plethora of information that is

stored on the device. Such information includes email accounts, phone numbers, calendar information, network or login credentials, confidential notes or files, and contact lists to name a few.

Fischer, Kuo, and Huang [6], discuss three shifts in mobile device security. The first is mobility, which created uncertainty about the mobile device surroundings. Mobile devices can be used on both secure and unsecure environments. For instance, connecting to public Wi-Fi at hotel is an example of an unsecure network, whereas, connecting to a work or personal network are usually secure. When users connect to an unsecure network, devices are open for attack. The second shift in security deals with sensors that are installed on the device. Most mobile devices have location tracking, Bluetooth, RFID, and cameras built-in. The automatic installation of sensors on mobile devices has led to a new area for attack. The final shift is constant connectivity. Mobile devices have constant access to the Internet and other devices, which is also attractive to cyber criminals.

The fact that mobile devices are portable makes them easy to steal. The owner of a stolen phone can actually lose all of their personal data [16]. People take the time to lock the doors to their homes and cars in order to provide security so that their personal property is not burglarized. But when it comes to securing mobile devices, that same care is often ignored. Most people would not walk down the street and hand their purse or wallet to a complete stranger to hold for 60 seconds or more. Yet the same people that would not turn over their purse or wallet will think nothing of asking a stranger to take a picture of them using their personal mobile device that contains a plethora of private information. People must take the time to implement physical security features as well as virtual security features in order to stay secure.

To begin to study mobile malware, it is useful to understand the category groupings used to describe different types of malware programs. Though different authors define these groupings in different ways, several common categories appear throughout the literature. These categories include viruses, worms, rootkits, botnets, phishing, spyware, Wi-Fi and Bluetooth hijacking, and malicious apps [11, 12, 13]. Each of these common categories will be briefly described.

A *virus* is a computer program that can replicate itself. Viruses are often programmed to infect other programs or files by attaching to them. A *worm* is a virus that copies itself and attempts to spread to other devices, typically through email messages in the desktop landscape, but also through Short Message Service (SMS) or Multimedia Message Service (MMS) messages, hereafter jointly referred to as "text messages" in order to travel from one mobile device to another [10]. A worm is similar to a virus, but does not have to attach itself to a program or file. Rather, it uses computer networks, including Wi-Fi, to spread to other devices, typically capitalizing on security flaws on the receiving device in order to access it. *Rootkits* infect the operating system (OS) of a device to allow viruses and other malware to hide in plain sight, stealthily disabling security features or overwriting OS files in order to remain undetected on the device for longer periods of time [11].

A *botnet* refers to a group of devices that have been compromised by malware that gives a hacker the ability to control the devices remotely. A hacker typically activates these "zombie" devices in concert to send spam, carry out Denial-of-Service (DoS) attacks, or perform other malicious acts. Attackers can also use mobile "zombie" networks to send text messages to premium numbers, incurring charges to the user for each message sent. Hackers often work with premium number service owners and receive a percentage of the money generated through these scams [11, 12, 14, 15].

Phishing scams, in which scammers pose as legitimate companies in order to swindle unsuspecting users into paying money or revealing private information, are much the same on mobile devices as they are on desktop platforms. However, in addition to email and social media posts, mobile phishing scams utilize text messages as well. *Smishing* is a term used to describe the exploitation of text messages on mobile devices for phishing scams [19].

Spyware applications are becoming common ground for cyber criminals to capture information. As previously mentioned, criminals have much to gain from accessing the information stored on mobile devices. Spyware applications monitor device communications, such as phone conversations, emails, text messages, inbound and outbound call logs and user locations. It is even possible for an attacker to listen remotely to phone conversations [9] or read text messages and emails. In fact, mobile spyware can also turn on a compromised smartphone without ringing, essentially turning it into a hidden microphone to eavesdrop on nearby conversations. The GPS functions of

the device can also be used to track its current location [12]. Most spyware applications can usually be detected provided that anti-malware applications are installed on the device.

Wi-Fi hijacking or *Wi-Fi snooping* occurs when hackers are able to intercept communications between smartphones and unsecured Wi-Fi hotspots, just as they can with desktop or laptop computers. This approach is called a man-in-the-middle attack, because everything that you type and transmit is intercepted by the hacker (the middle man) before it gets to where it was intended. This means that a hacker could easily gain access to usernames, passwords, and even credit card information if a user logs in to web sites or purchases items online while being monitored [2, 3]. For convenience, many smartphones have settings to allow the device to automatically connect to available Wi-Fi networks, making the device vulnerable.

Bluetooth, one of the most common short-range wireless protocols, is often used to allow connectivity between mobile devices. There are a few different types of vulnerabilities that can be exploited when Bluetooth connectivity is turned on for a mobile device. *Bluejacking* is a type of practical joke akin to spam. A Bluejacker can send an e-contact card to another Bluetooth device in discoverable mode, as long as it is within approximately a 30-foot radius of their own device. However, instead of adding a real contact into the unsuspecting recipient's smartphone, the Bluejacker exploits the e-contact card to replace the "From" section with a message. When the recipient receives this "Bluetooth spam," it can often scare the person into realizing that they are under surveillance, which is typically the intention of the Bluejacker. *Bluebugging* allows a hacker to gain access to another user's device through Bluetooth and control some of its functions, including making phone calls or sending text messages to premium numbers or eavesdropping on calls made by the user [18].

Hackers can also compromise smartphones and other mobile devices by embedding malware into mobile apps that users then download and install. These malicious apps are often free in order to entice users to download them, and once installed they can steal private information from the device and send it back to a hacker. They may also install other apps or open "backdoors" on the device, allowing a hacker to take remote control of the device at a later time [12].

PURPOSE OF STUDY

The literature examined makes it clear that mobile malware is on the rise. It also points out a variety of ways in which mobile device security measures parallel the security measures of standard computers. For example, mobile malware spreads in much the same way as viruses spread between computers: via email attachments, phishing web sites, exploitation via public Wi-Fi networks, infection of seemingly official programs (apps), text messages, Bluetooth connectivity, and physical theft or intrusion. Simple steps can be taken to protect mobile devices from much of the threat of mobile malware, if people are aware that a smartphone must be protected from malware. This exploratory study sought to explore awareness, concern and usage habits of mobile security protection measures among university students and alumni.

The following research questions were addressed:

RQ1: Do university students and alumni demonstrate awareness of mobile malware risk factors by using preventative security measures to mitigate mobile malware risk factors for mobile devices?

RQ2: Is there a relationship between concern about mobile malware and preventative security measures used by university students and alumni?

RESEARCH METHODOLOGY

This exploratory study examined awareness, concern and use of security measures for protecting mobile devices against mobile malware among university students and alumni. An electronic survey was distributed to a convenience sample of undergraduate students, doctoral students, and doctoral alumni at a mid-Atlantic university during March and April 2014. Undergraduate students in the sample were selected from course sections in the Computer Information Systems department that were required as part of the university core or were electives known to be taken often by non-majors as well as majors within the department. These selections were made to attempt to capture a cross-section of students from various fields of study within the university within the convenience sample. Doctoral students and doctoral alumni of the university were also included in the sample, as these individuals are a diverse group in terms of age, ethnicity, location, occupational affiliations. Again, these participants were selected purposefully in order to capture a cross-section of individuals from a variety of industries and backgrounds. As this research is exploratory in nature, and very few previous studies addressing mobile malware and security awareness were found, the researchers wished to include as much diversity in the sample as possible. The survey was administered to 138 undergraduates and 76 doctoral student and alumni. Participants were first asked if they owned a smartphone or tablet. Any participants who did not own a smartphone or tablet exited the survey, and these responses were discarded. After participants without a mobile device were removed from the data set, there were 114 undergraduate and 73 doctoral student and alumni responses, for a total of 187 participants. Prior to survey administration, a pilot test was conducted with 61 adult participants to test the validity and reliability of the survey questions.

The survey questionnaire consisted of a variety of questions relating to mobile security protection measures. Participants were first asked some basic demographic questions including age, gender, and occupational affiliation. Next, participants were asked about the types of smartphones and tablets that they own, including device platforms such as iOS, Android, BlackBerry, Windows Phone, Symbian and Other for smartphones and iOS, Android, Kindle and Other for tablets. Then, participants were asked about their habits regarding the downloading of mobile apps, including whether they had ever downloaded an app, how often they download free and paid apps, and how often they download financial, health-related, social media, and productivity apps. These four categories of apps were chosen because of the sensitive nature of the data that is typically stored in these types of apps.

The next set of questions was targeted toward understanding the participants' usage habits regarding several mobile security risk factors identified from the literature. Participants were asked if they typically read reviews before downloading apps, which can be a significant deterrent to downloading malicious apps [4]. They were also asked if they had ever used an anti-virus or anti-malware app on their device, which can work much like their desktop computer counterparts to scan for viruses and malware [12]. Next they were asked if they typically leave Bluetooth "on" on their mobile device, if their device is set to automatically connect to Wi-Fi networks and how often they connect to public Wi-Fi hotspots, all of which are risk factors for hijacking and man-in-the-middle attacks [2, 3,16, 18]. Next the questionnaire covered security measures for protecting against unauthorized physical device access, damage or loss. Participants were asked if their device is locked with a password, PIN or fingerprint and also about the frequency with which they backup data from their device. Physical locks and backups are important security measures, as the most common method of information theft from a mobile device involves physical theft of the device [17]. Care was taken that some of the questions were negatively worded while others were not, so as to not skew the results. For instance, one question was worded "Do you typically read reviews or otherwise research a mobile app before downloading and installing it?" A "Yes" answer to this question reveals that the user does not have a risk factor in this category because reading reviews can be a significant deterrent to downloading malicious apps. Another question was worded, "Is your mobile device set to automatically connect to WiFi hotspots?" A "Yes" answer to this question reveals that the user does have a risk factor as his or her device could autoconnect to unsecured Wi-Fi networks.

The next set of questions was focused on participants' awareness of mobile security risk factors. Participants were asked if they had ever experienced a virus or malware on their mobile device, and also whether they were concerned about viruses or malware in regard to their mobile device. Lastly, several questions relating to information privacy concerns were asked, but not utilized for this study.

FINDINGS

Of the 187 participants, 66% were male and 34% were female. The age range of participants spanned from 18 to 72, with a mean of 32. The largest age group represented included 18-20 year-olds, at 31% of the sample. Participants aged 21-30 made up 25% of the sample, those aged 31-40 made up 11%, those aged 41-50 made up 18%, those aged 51-60 made up 10%, and the remaining 5% included participants aged 61-72. The slight skew toward the younger end of the age spectrum can be largely attributed to the 114 undergraduates included in the sample. In terms of occupational affiliation, 36% of participants worked in industry (for profit), 3% worked for a non-profit organization, 10% worked for government (local, state or federal), 4% worked in health care, 30% worked in education, and 17% indicated "other." Nearly all of the responses in the "other" category came from undergraduates and can perhaps be attributed to the fact that many undergraduates were not working while attending school. In retrospect, a "not applicable" category would have been useful to add to this question.

All participants who were kept in the data set owned at least one mobile device. A majority of the participants, 94% owned a smartphone and 63% owned a tablet. Nearly all of the participants, 96%, had downloaded a mobile app to their device. Of those who had downloaded a mobile app, the majority tended to download free apps more frequently than paid apps. More than half, 53%, downloaded free apps frequently or very frequently, 40% occasionally, 6% rarely, and 1% never. Only 7% downloaded paid apps frequently or very frequently, 19% occasionally, 43% rarely, and 31% never downloaded a paid app. Regarding types of apps downloaded, participants who had downloaded an app were asked how often they downloaded financial, health-related, social media, and productivity apps, since these categories of apps are the most likely to involve the use of private information. For financial apps, 39% downloaded them frequently or very frequently, 17% occasionally, 15% rarely, and 29% never. For health-related apps, 21% downloaded frequently or very frequently, 28% occasionally, 17% rarely, and 34% never. For social media apps, 71% downloaded frequently or very frequently, 13% occasionally, 10% rarely, and 6% never. And lastly for productivity apps, 36% downloaded frequently or very frequently, 28% occasionally, 18% rarely, and 18% never.

Participants were directly asked whether they were concerned about mobile malware in regard to their mobile devices. The sample was nearly split evenly, with 46% responding that they were concerned, 50% responding that they were not concerned, and 4% responding "I don't know," which could indicate a lack of awareness of the topic. The concern about mobile malware was relatively high given that very few of the participants, 2%, had experienced mobile malware on their own device. The majority, 88%, indicated that they had not experienced mobile malware. However, 10% responded "I don't know" to this question, which can be construed as a general lack of awareness regarding mobile malware. These percentages are depicted in Figure 1.

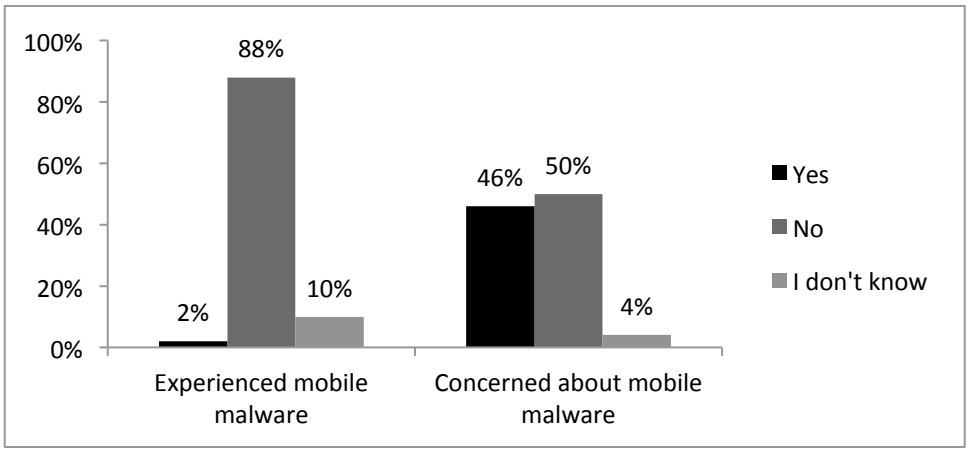

Figure 1. Percentage of participants who experienced and are concerned about mobile malware

RQ1 asked, "Do university students and alumni demonstrate awareness of mobile malware risk factors by using preventative security measures to mitigate mobile malware risk factors for mobile devices?" To answer this question, the researchers looked at the responses to seven questions on the questionnaire that each demonstrated a risky behavior in terms of preventative measures for mitigating exposure to mobile malware. These seven questions included asking participants how often they use public Wi-Fi, whether their device is set to autoconnect to Wi-Fi networks, whether they typically leave Bluetooth connectivity set to on, whether they read reviews before downloading apps, if they have ever used anti-malware on their device, how often they backup data on their device, and whether they lock their device with a password, PIN or fingerprint.

The majority of participants displayed risky behavior in terms of connecting to public Wi-Fi networks, with 73% indicating that they connect to public Wi-Fi occasionally or more frequently, while 26% indicated that they rarely or never connect to public Wi-Fi. When asked if their mobile device is set to automatically connect to Wi-Fi hotspots, the majority of participants, 70%, displayed non-risky behavior by indicating that they do not allow their device to automatically connect to Wi-Fi. Of the participants displaying risky behavior for this question, 26% indicated that they do have this setting, while 4% answered "I don't know."

Thirty-one percent (31%) of participants indicated that they do leave Bluetooth on or that they did not know, both indicating risky behavior. The remaining 69% responded that they do not leave Bluetooth on.

The majority of participants, 72%, indicated that they do read reviews or otherwise research a mobile app before downloading and installing it, displaying non-risky behavior. The remaining 28% did not read reviews, thus making their devices more vulnerable to downloading malicious apps. However, most participants, 75%, displayed risky behavior by failing to use anti-malware software or apps. Sixty-six percent (66%) had never used anti-malware, while 9% indicated that they did not know if they had or not, also a risky behavior indicating a lack of awareness of anti-malware. Only 25% of participants had used anti-malware.

In terms of physical security preventative measures, 73% of participants responded that they backup data on their mobile devices occasionally or more frequently, while 27% backup rarely or never. The majority of participants, 77%, protect their devices with a password, PIN, or fingerprint while the remaining 23% do not.

RQ2 asked, "Is there a relationship between concern about mobile malware and preventative security measures used by university students and alumni?"

To answer this question, the researchers created a Mobile Malware Risk Factor Index based on the seven mobile malware risk factors questions utilized to answer RQ1. The development of an index is a supported way to measure a construct using an accumulation of scores from a variety of related but individual items [1], and is often done to transform data into a form that can be used in other statistical analyses.

To build the index, the response to each of these seven questions was scored one (1) if the response indicated a risky behavior including using public Wi-Fi occasionally or more frequently, leaving their device set to typically keep Bluetooth connectivity on, using a device setting to allow autoconnecting to Wi-Fi networks, not reading reviews or researching apps before downloading them, not using anti-malware on their device, backing up their device data rarely or never, or not locking their device with a password, PIN or fingerprint. Responses that demonstrated non-risky behaviors (the opposites of those mentioned) were scored a zero (0). The scores were then summed to build a Mobile Malware Risk Factor Index that ranged from zero (the least risky) to seven (the most risky).

The relationship between concern about mobile malware and mobile malware risk factors (as measured by the Mobile Malware Risk Factor Index) was investigated using the Pearson product-moment correlation coefficient. Preliminary tests were performed to ensure that the assumptions of normality, linearity and homoscedasticity were not violated. There was a significant, negative correlation between the two variables with a small effect size, $r = -.191$, $n = 177$, $p < .05$, with high levels of concern associated with lower levels of risk factors.

LIMITATIONS

The primary limitation of this study was its small sample size, using a convenience sample at a single university. The researchers encourage future studies to incorporate participants from multiple universities or geographic regions. Although the sample population of the study is small, the findings are still relevant to area of mobile security and will assist with future research on the topic.

CONCLUSIONS

Overall, the participants surveyed in this study proved to be relatively savvy in terms of use of preventative measures regarding mobile malware in regard to autoconnecting to Wi-Fi networks, leaving Bluetooth connectivity on, reading reviews before downloading mobile apps, regularly backing up device data, and using a locking mechanism such as a password, PIN or fingerprint to control access to their device. These are very encouraging results. However, the sample did not demonstrate awareness of the risks of connecting to public Wi-Fi networks, and did not indicate much use of anti-malware software or apps to protect their devices.

In addition, a significant, negative correlation, $r = -.191$, $n = 177$, $p < .05$, was found between concern about mobile malware and mobile malware risk factors as measured by the Mobile Malware Risk Factor Index that was constructed as a composite score from seven items on the survey questionnaire. This means that participants who were more aware and concerned about mobile malware were more likely to display fewer risk factors. This may indicate that participants who were not concerned about mobile malware may have been unaware of the tested risk factors. Also, it should be noted that several questions were answered by participants in ways that suggest there may be confusion about some of the risk factors, such as responding "I don't know" when answering the questions. The results of this study are mixed, but with mobile malware clearly on the rise, further attempts to raise awareness of mobile malware risk factors can only serve to aid mobile device users.

The following list of recommendations can help mobile devices users to stay secure in terms of mobile malware:

1. Lock your mobile device with a password, PIN or fingerprint to protect it from physical access.
2. Cover the device when typing in the PIN or code because one never knows who might be watching.
3. Maintain physical control of the device. Never hand the device to someone to take a picture or rest it on the counter at a store when making a payment.
4. Research the features of your mobile device. Often times, people are unaware of the capabilities of their devices. Many have password features that will automatically lock the phone if the incorrect password has been entered three times. A four or five digit PIN is then required to access the device (Ruggiero, 2013).
5. Install malware/security applications to regularly scan your device.
6. Back up the data on all mobile devices on a regular basis.
7. Check monthly phone bills for unusual activity.
8. Do not automatically connect to public Wi-Fi. Hackers can utilize man-in-the-middle attacks or create fake Wi-Fi hotspots to fool unsuspecting users.
9. Turn Bluetooth to "off" when not in use and set Bluetooth-enabled devices to non-discoverable. This makes the device invisible to others.
10. Carefully decide what type of information to store on your mobile device. Refrain from storing passwords, bank account information or personal security information.
11. Refrain from installing mobile apps without conducting research, especially in regard to free apps or apps sold in unregulated third-party app stores.
12. Delete all information stored on the device before donating or throwing it away.

REFERENCES

1. Babbie, E. (2001). The Practice of Social Research: 9th Edition. Belmont, CA: Wadsworth Thomson.
2. Bharti, A. K., Goyal, M., & Chaudhary, M. (2013). A Review on Detection of Session Hijacking and Ip Spoofing. *International Journal of Advanced Research in Computer Science*, *4*(9).
3. Escobar, E. (2013, March 6). The dangers of unsecured Wi-Fi hotspots. Retrieved May 2, 2014, from Quick and Dirty Tips website: http://www.quickanddirtytips.com/tech/mobile/the-dangers-of-unsecured-wifi-hotspots
4. Fedewa, J. (Ed.). (2014, May 6). Android antivirus: 6 truths about smartphone malware. Retrieved May 8, 2014, from Phandroid website: http://phandroid.com/2014/05/06/android-virus-malware-scan/
5. Felt, A. P., 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. 3-14). ACM.
6. Fischer, I., Kuo, C., & Huang, L. (2012). Short Paper: Smartphones: Not Smart Enough? *SPSM'12,* October 19, 2012, Raleigh North Carolina. Retrieved on May 2, 2014 from http://www2.berkeley.intel-research.net/~hling/research/spsm12.pdf
7. Frost & Sullivan. (2013). The many shades of mobile app risk: understanding and mitigating mobile threats effectively. Retrieved on May 8, 2014 from http://www.brightcloud.com/pdf/MobileSecurity-Webroot-20131021110609-43358.pdf
8. GSMA Intelligence (2014). Global mobile penetration – subscribers versus connections. Retrieved on May 3, 2014 from https://gsmaintelligence.com/analysis/2012/10/global-mobile-penetration-subscribers-versus-connections/354/
9. Juniper Networks. (2011). Mobile device security- emerging threats, essential strategies. Key capabilities for safeguarding mobile devices and corporate assets. White paper. Retrieved on March 5, 2014 from http://www.juniper.net/us/en/local/pdf/whitepapers/2000372-en.pdf
10. Kirk, J. (2014, April 30). Worm-like Android malware spreads using text messages. Retrieved May 2, 2014, from PC World website: http://www.pcworld.com/article/2150400/wormlike-android-malware-spreads-using-text-messages.html
11. La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. IEEE Communications Surveys & Tutorials, 15(1), 446-471.
12. Leavitt, N. (2011). Mobile security: finally a serious problem?. *Computer*, *44*(6), 11-14.
13. Malware - definition, history and classification. (n.d.). Retrieved April 10, 2014, from BullGuard Security Centre website: http://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx
14. Panda Security. (2013, April-June). Quarterly Report Pandalabs. Retrieved on April 22, 2014 from http://press.pandasecurity.com/wp-content/uploads/2010/05/Quarterly-Report-PandaLabs-April-June-2013.pdf
15. Patten, K. P., & Harris, M. A. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. *Journal of Information Systems Education*, *24*(1).
16. Ruggiero, P., & Foote, J. (2011). Cyber Threats to Mobile Phones. U.S.-CERT. United States Computer Emergency Readiness Team. Carnegie Mellon University. Retrieved on April 29, 2014 from https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf
17. Skoudis, E. (n.d.). Defining mobile device security concerns. Retrieved May 9, 2014, from SearchSecurity website: http://searchsecurity.techtarget.com/answer/Defining-mobile-device-security-concerns
18. Stern, A. (2013, April 15). Bluetooth connectivity threatens your security. Retrieved March 5, 2014, from Kaspersky Lab website: http://blog.kaspersky.com/bluetooth-security/
19. US CERT. (2010, April 15). US-CERT Technical Information Paper – TIP-10-105-01. Retrieved on May 3, 2014 from https://www.us-cert.gov/sites/default/files/publications/TIP10-105-01.pdf
20. Webroot. (2013). Mobile Threats are Real and Costly. A commissioned study. Retrieved on April 16, 2014 from http://www.webroot.com/shared/pdf/byod-mobile-security-study.pdf