https://doi.org/10.48009/4_iis_2016_246-253

Issues in Information Systems
Volume 17, Issue IV, pp. 246-253, 2016

DOWNLOADING MOBILE APPS: ARE STUDENTS AWARE OF THE SECURITY RISKS?

Adnan A. Chawdhry, California University of PA, chawdhry_A@calu.edu
Karen Paullet, Robert Morris University, paullet@rmu.edu
David M. Douglas, Robert Morris University, douglas@rmu.edu
Joseph Compomizzi, Florida Atlantic University, jcompomizzi@fau.edu

ABSTRACT

Mobile applications (apps) are taking the world by storm. Currently, end users have downloaded over 225 billion apps on their mobile devices. Security concerns surrounding the downloading of apps are often overlooked. The apps on our smart phones can be accessed by the tip of our fingers or the sound of our voice. One must think about the interactive risks to our privacy and the security concerns that can affect our digital lives. This study explores awareness and security risks associated with downloading mobile apps. A total of 124 students were surveyed at two mid-Atlantic Universities. The study found that many students are downloading mobile apps without fully understanding the security risks associated with such action.

Keywords: Mobile Security, Mobile Applications, Apps, Mobile Device

INTRODUCTION

Mobile applications could be considered a scourge or savoir to human interaction with our smart phones depending on who is asked. Each day many new or improved mobile applications are being created. These App creators can be found in all age groups, cultures and from all social economic backgrounds. Some are designed to make our life easier (location and directional) and less stressful (reminders and flashlight). It appears there is an App for all needs both real and perceived. According to Statistica (2016), there has been an upward trend in mobile app usage. In 2011, there were 22 billion free app downloads and 2.9 billion paid app downloads. As of June 2016, people have downloaded over 211 billion free apps and 13.49 billion paid apps showing the significant rise in mobile app usage.

These App creators, both young and old create for fun, profit, or perhaps most importantly to fill a "void" in the ever expanding catalogue must have "apps." These apps, also known as mobile applications, are designed, or so they say, to improve our lives. Perhaps they do in some respect, but one of the unintended consequences is a more complacent and indolent mobile community especially in regards to cyber security and the oversharing of information both private and public.

However as with all things in life, there are unintended consequences. We live in a brave new world of the Internet of Things (IoT) and smart phones. The applications (Apps) on our smart phones are at the tip of our fingers or the sound of our voice. Knowing and unknowingly we often overshare many aspects of our personal information in cyberspace. Once shared, we can never retrieve or change this cyber data. The information is now beyond our grasp and control. One wrong click or one wrong tap of our finger on the wrong button or link can change a life instantly. This lapse of judgment or mistaken "click or send" can allow a miscreant hacker or rouge agency to gain access to financial and personal aspects of our digital lives. One must think about the interactive risks to our privacy and the security concerns that can affect our digital lives. The following questions were explored.

1. Are students aware of privacy / security concerns when downloading applications on their mobile devices?

2. Is there a statistical significance among age, gender, and level of education with student's awareness of privacy / security with downloading applications?

LITERATURE

The rapid growth of mobile services is calling for a deeper look at technology and its operations for users. The terms "mobile technology" or "mobile devices" which formerly were synonymous are taking different meaning for users which impact the applications these operators choose, the interfaces with which they exchange, and the functions they transact. Hence the terms "mobile technology" and "mobile devices" are requiring closer examination. This examination is revealing a difference in the perception of "mobile" means. A 2014 study by the organization, Salesforce, on the behaviors of mobile technology users is disclosing, more clearly, this differentiation observed by mobile technology operators. In their Mobile Behavior Report, Salesforce found that 54% of 470 voluntary mobile technology consumers associated "mobile" specifically with a smartphone or cell phone (2014). Conversely only 14% identified the term "mobile" with tablets or readers in the Salesforce study. Noteworthy, this difference in perception led the Mobile Behavior study to conclude that users inferred that "mobile" means ease of use and on the go with consumers demonstrating "a strong link between that device that is their pockets and the connected freedom it brings" (Salesforce).

Tablets, on the other hand, are identified more as companions to the smartphones and cell phones for which users indicated that "the tablet isn't truly a mobile device. Instead, it's a largely in-home device that lends itself well to cross-device usage mostly employed by people earning $75,000-$100,000 annually and aged 35-44 years" (Salesforce, 2014).

These statistics regarding the users of mobile technology and the number of devices sold is leading to an abundance of research regarding their use. Importantly, regardless of the device model, mobile technology, specifically smartphones and tablets, are dependent on functionality with third party applications in addition to operating platforms such as Apple's iOS and the Ardoid 6.0 Marshmallow. These interfaces between the operating systems and applications provide the ease of use and computing freedom that mobile operators perceive as the technology's greatest benefits. A 2013 study by Compomizzi regarding iPad use by military and U.S. veteran college students revealed that 71.1% of respondents indicated that the device was easy to use and increasingly useful for academic tasks and social interaction. In fact, the study also revealed that 29.8% of participants who strongly agreed that the iPad was a useful academic tool had GPA's between 3.1 and 4.0. Salesforce's 2014 study disclosed that 90% of participants ages 18-24 indicated that "mobile devices are a central part of everyday life" on the average spending 3.3 hours per day on a smartphone (Compomizzi, 2013).

Koved, Trewin, Swart, Singh, Cheng, Chari (2013) discussed the risks associated with the adoption of mobile devices regarding its authentication and authorization on network services. Their research especially focused when these devices were relied on to input or share sensitive information. Mobile devices such as smartphones, tablets, and other "mobile platforms" are now commonly used for banking and shopping. Accordingly they have identified several risks. They include the possibility of that the user's action will be observed and allow an unauthorized authentication or "impersonation" on a different device. Understandably, when devices are stolen or lost the risks of exposing sensitive information is increased. "In particular, mobile device applications, including the web browsers, are caching authentication credentials, enabling an attacker to exploit them. Modern smartphones can enable multi-factor authentication by using sensors such as cameras and microphones to capture biometric data" (Koved, 2013).

Concerning third party applications commonly referred to as mobile apps, distribution marketplaces such as Apple's App store offer two types: paid apps and free apps. Understanding the difference between the two provides a foundation to pivot a discussion on security issues with mobile technology devices. Free apps, with no surprise, are more popular than paid apps. According to Petsas, Papadogiannakis, Polychronakis, Markatos and Karagiannis (2013), "paid apps usually have more advanced functionality and do not include advertisements" (p. 285). According to the study conducted by Compomizzi (2013), of the college student participants with iPads, 54.2% indicated that they paid for a few apps while 20.5% indicated that they didn't pay for any. Further, participants in this study indicated that the apps they purchased were related to academic uses specifically to complete study tasks like note-taking app's, for academic tools like calculator and dictionary apps, and for course requirements like e-book apps and video apps.

Given that free apps rely on advertisements, learning about the usage patterns by mobile device operators yields additional information that leads to a more thorough examination of the issue of security. In the study by Petsas, et al. (2013), 55,000 free apps from the Google Play Store were categorized, tracked and examined. The analysis of data collected in the study disclosed that the top 10 categories accounted for 60% of the apps. These app categories included tools, entertainment, brain apps like puzzles, lifestyle, business, books, travel, education and casual. Of the 55,000 apps examined, 46,000 as for the android permission to access the network. Further, of these 46,000 apps, 19,000 were connected to at least one advertisement library (Petsas, 2013).

The connections with advertisement libraries allow user behaviors to be examined. For example, as Petsas et al. (2013) points out a study of the user behaviors with activity recorded with the advertisement libraries enables better prefetching, which in turn transfers data from memory to temporary storage for later use. The understanding of user downloads patterns also aids in building more complicated recommendation systems. As Petsas et al. explain: recommendation systems utilize collaborative filtering methods in which groups of users who share similar interests based on download patterns are identified. Analysis of these patterns then enables suggestions for other services and products such as other apps, coupons, and emails from brands or retailers. According the 2014 Mobile Behavior Report, 64% of consumers reported that they subscribe to brand email notification services because the deals offered, the appeal of being updated on products and services, quick access to information, meaningful content or the lack of desire to visit the business website or app for information or purchase (p.19).

With this understanding of mobile technology, system operations, user behaviors, and app interfaces, Theoharidou, Mylonas, and Gritzalis (2012) explain the mobile apps are both an asset and threat for users. While the social, financial and business benefits of an app are numerous, the app itself may need protection and can act as a security attack access point for users. These security threats range from spoofing, to cloning, to unauthorized access, to disablement, to phishing to malware injection all related to permission access rights and authentication violations (Theoharidou, Mylonas, and Gritzalis, p. 450). As Koved, Trewin, Swart, Singh, Cheng, and Chari (2013) write, "In particular, mobile device applications, including the web browsers, are caching authentication credentials, enabling an attacker to exploit them" (p. 1).

The good news is that advances in mobile technology and user protection continue in development. Secure passwords are only the beginning. Mobile and smart technology are incorporating camera and voice detection sensors. Biometrics with fingerprinting and retinal recognition are also advancing to counteract privacy and security concerns. The bad news is that these additional security features are often in direct contrast to mobile operators' expectations of easy to use, fast, and on-the-go technology. Users often view these additional security steps as burdensome. In a study conducted with IT professionals who also teach at the college level by Compomizzi, D'Aurora, and Rota (2013), of 90 question responses received regarding security practices, 76 indicated regular practice of low tech methods of protection such as password authentication and using multiple browsers for different computing functions while only 14 employed high tech methods of security protection like biometrics.

The literature concerning how mobile technology is perceived and used by operators is ever-growing. Interesting definitions of a mobile device continue to emerge. Likewise, the uses of mobile technology continue to grow, placing demand upon more flexible, available and integrated computing capabilities and mobile applications. With this expansion in mobile technology, security risks are also increasing. While software and hardware developers forge ahead with progressed security solutions, users may perceive them as burdensome; thereby opening the door to information invasion and attack.

RESEARCH METHODOLOGY

The study surveyed students from two small mid-Atlantic Universities from March to April 2016. For this study, the population chosen comprised of undergraduate and graduate students enrolled in on-campus or online programs. This population was chosen to ensure students surveyed would be 18 years or older. A total of 124 students completed the survey. The researchers utilized Survey Monkey, an online survey tool, to collect data, which were then imported into SPSS for organization and analysis. As part of the analysis, the researchers used a Chi-square

analysis with a statistical significance at the .05 margin of error with a 95% confidence level. The study addressed the following two research questions.

1. Are students aware of privacy / security concerns when downloading applications on their mobile devices?
2. Is there a statistical significance among age, gender, and level of education with student's awareness of privacy / security with downloading applications?

The survey administered to students consisted of 22 closed-ended questions and one open-ended question for further understanding of the participants responses. The first three questions focused on student demographics to include age, gender, and level of education. The remaining questions focused on whether students were aware of security and privacy concerns that exist with downloading mobile applications. The questions primarily focused on responses of "Yes" and "No", while a few questions provided additional options for students to select the type of mobile device they use, applications they use on their phone, and how many apps they have downloaded.

RESULTS

The survey presented eight scenarios where it prompted the participant to respond with a "Yes" or "No" answer. These questions were designed to understand the student's level of awareness with mobile application security and privacy in addition to providing input for the researchers to understand what actions they perform with their mobile phones. These questions included knowledge of downloading mobile applications, disabling location services, clearing browsing / search history, backing up photos, apps, and contacts using a third party app, and installing anti-malware software. Additionally, it asked supplemental questions to understand if students were aware that downloaded applications can have access to your phones content. The summary of these results are provided in Table 1. Additionally, you will find a chi-square analysis performed on these participant responses against age, gender, and level of education to understand any statistical correlation that may have existed. Only values of .05 or less were considered statistically significant. These results can be found in Table 2.

Table 1. Mobile Phone Settings

	Yes	**No**
Downloaded Mobile Apps	96.64%	3.36%
Disabled Location Services	84.48%	15.52%
Clear Browsing / Search History	74.14%	25.86%
Backup using 3rd Party Software	34.21%	65.79%
Installed Anti-Malware	29.31%	70.69%
Aware that Apps have access to phone content	85.34%	14.66%
Read Terms of Use	34.48%	65.52%
Lost / Stolen Phone	14.16%	85.84%

Table 2. Chi-Square Analysis

	Age (df = 6)	Gender (df = 1)	Level of Education (df = 5)
Use a Mobile phone on a regular basis	0.152	0.386	0.457
Disabled Location Services	0.704	0.362	0.98
Clear browsing / search history	0.016	0.035	0.234
Backup phone contents with third party app	0.05	0.925	0.506
Use anti-malware	0.028	0.002	0.234
Aware that downloaded app provider has access to content on phone	0.713	0.013	0.189
Read Terms of use / service	0.197	0.201	0.249
Phone been lost / stolen	0.49	0.008	0.48

Additionally, the researchers were interested to further analyze the student responses on reading the terms of use for an application compared to their awareness that applications have access to their phone's content. Approximately 83.19% of the students were aware that mobile applications have access to their content while only 14% were unaware of this. Additionally, only 33.61% of students responded that they have read the terms of use before downloading an app. The highest percentage of 51.26% was found where students did not read the terms of use but were aware that applications have access to their phones content. The breakout of these results can be found in Table 3.

Table 3. Reading Terms of Use vs Awareness of App Access

		Aware that Apps have access to phone content		
		Yes	No	**Total**
Read Terms of Use	Yes	32.76%	1.72%	34.48%
	No	52.59%	12.93%	65.52%
Total		85.34%	14.66%	100.00%

For further analysis, the researchers also asked each participant of their mobile device choices to identify a potential trend among various demographics. The mobile device choice was analyzed against the participant's age, gender, and level of education. From the results, it was noted that 53.72% of the overall users utilized an iPhone, 38.84% had an Android device, 6.61% chose an iPad, and .83% chose other. The breakout of these results against the demographic characteristics can be found in Tables 4-6.

Table 4. Age vs. Mobile Device Choice

Age	iPhone	iPad	Android	Other	Total
18-25	42.22%	4.21%	29.11%	0.00%	75.54%
26-35	3.54%	0.00%	3.54%	0.00%	7.08%
36-45	0.88%	0.00%	3.54%	0.00%	4.42%
46-55	4.42%	1.52%	1.77%	0.83%	8.54%
56-65	0.88%	0.88%	0.88%	0.00%	2.65%
66-75	1.77%	0.00%	0.00%	0.00%	1.77%
Total	53.72%	6.61%	38.84%	0.83%	100.00%

Table 5. Gender vs. Mobile Device Choice

Gender	iPhone	iPad	Android	Other	Total
Male	26.45%	1.65%	28.93%	0.00%	57.02%
Female	27.27%	4.96%	9.92%	0.83%	42.98%
Total	53.72%	6.61%	38.84%	0.83%	100.00%

Table 6. Level of Education vs. Mobile Device Choice

Level of Education	iPhone	iPad	Android	Other	Total
Undergraduate Freshman	5.79%	0.00%	2.48%	0.00%	8.26%
Undergraduate Sophomore	8.26%	0.00%	8.26%	0.00%	16.53%
Undergraduate Junior	14.88%	2.48%	4.96%	0.00%	22.31%
Undergraduate Senior	10.74%	1.65%	12.40%	0.00%	24.79%
Graduate Masters	9.92%	1.65%	4.13%	0.83%	16.53%
Doctorate	4.13%	0.83%	6.61%	0.00%	11.57%
Total	53.72%	6.61%	38.84%	0.83%	100.00%

Finally, the researchers wanted to understand what applications / functions were being used by the participants. The survey provided a finite list of values and asked the participants to choose multiple values representing which applications / functions they currently use on their mobile device. Each of the applications had a 50% or higher response with the exception of reading books. The top three applications / functions used were Email at 91.13%, Information Search at 84.68%, and Music at 81.45%. The complete set of responses can be found in the Table 7.

Table 7. Applications / Functions Used

Application / Function	Total
Facebook	70.16%
Twitter	50.00%
Instagram	56.45%
Snapchat	62.10%
Email	91.13%
Games	56.45%
Music	81.45%
Books	31.45%
Information Search	84.68%

DISCUSSION

A major part of awareness is educating people on the possible outcomes that arise from a single action. In this study, the researchers presented the participants with a number of scenarios that could present a security or privacy concern from using their mobile device. Surprisingly, 96.64% of the respondents stated that they have downloaded mobile applications on their device. Interestingly enough, 85.34% of the participants also knew that mobile applications have access to their phones content. This was shocking because a vast majority of the participants were aware of the security or privacy threats of downloading these applications but still chose to install them. A second component to this was to understand what settings users changed on their phone. Of the participants 84.48%

chose to disable locations services and 74.14% of the overall participants have cleared their browsing or search history. These results illustrated that participants did take some action on protecting themselves. However, only 29.31% of respondents had actually installed Anti-Malware software on their device, illustrating they were either unaware of such an application or felt it was not as important to their security or privacy.

Not so surprising, 34.48% of the respondents stated that they read the terms of use, while 65.52% stated they did not read it. The most interesting part of this response was when it was coupled with the question of the student's awareness that downloaded application providers can have access to your phone's content. Of the respondents 85.34% stated they were aware of this concern while only 14.66% stated they were not aware of it. Further breaking this down, the researchers found that of the 85.34% that were aware of application providers being able to access your phones content, 32.76% have read the terms of use while 52.59% have not. Since all terms of use documents are not the same, this was shocking because the results illustrated that even though the students knew of the concern, they still chose not to better understand the specifics of what content is accessed and how it will be used by the mobile application provider. One assumption is that the respondents have weighed the need for the application over the security or privacy concern and have accepted this risk while choosing to install the application. This assumption was made since over half of the respondents were aware that mobile application providers can access their content and have chosen not to read the terms of use.

One final component to consider when considering the respondents choice to download an application regardless of the security or privacy concern is the level of perceived protection with mobile devices. Many have argued that Apple's hardware and software are secure and applications go through a rigorous screening process before they are released to the public. For this reason, individuals may have chosen Apple devices over others for the perceived protection. Of the participants, approximately 60% chose an apple device (iPhone and iPad) while 38.84% chose an open-architecture Android device. The researchers thought that this could have possibly impacted the participant's choice to still download the mobile application after feeling a perceived sense of security with their device. However, after furthering analyzing a respondent's mobile phone choice versus their awareness of mobile applications content access, the researchers found that approximately 51% of the respondents had awareness and choice an Apple device and approximately 34% of the respondent's choice an android device and were aware of the risk. While a statistical significance did not exist between these two variables, one could still hypothesize that Apple users still downloaded applications knowing the security and privacy concerns since they perceived Apple to be a safer device. However, the researchers were unable to truly test this hypothesis given their restricted dataset.

Lastly, the researchers wanted to understand if there existed a statistical significance among the three demographics (age, gender, and level of education) versus the mobile phone settings that existed. Of the 8 scenarios, level of education did not have any statistical significance (a chi-square value of less than .05), while age had three and gender had four. For both Age and gender, the researchers found a statistical significance with clearing their browser / search history having chi-square values of .016 and .035, respectively. Using Anti-Malware software had a .028 chi-square value with age and a .002 chi-square value with gender. Additionally, age found another statistical significance with backing up the phone contents using a third party application while having a chi-square value of .05. While this was not statistically significant for gender, gender did have a statistical significance with their awareness of mobile applications providers having access to their phones (chi-square value of .013) and their phone being lost or stolen (chi-square value of .008).

CONCLUSION

Mobile application security awareness is a key factor of ensuring that end users make informed decisions in order to stay safe while using their mobile devices. Some users may do a comparison of the perceived benefits versus the assumed costs (security or privacy concerns) to determine whether or not the application provides value. Prior to downloading and application, end users should research the application by reviewing the security measures, end use agreement and checking the number of application downloads for the app. For instance, if the app has been downloaded by only a handful of end users could mean that it is not safe and has vulnerabilities. Popular apps will have a large download number. It would be interesting to know if the participants would have still downloaded the applications after they read the terms of use in its entirety. A question to ponder after the review of the study still sits

with whether or not users really care about security privacy concerns. The results of this study illustrated to the researchers that even though mobile users were aware of what application providers can access on their phone, they still were indifferent in terms of downloading the application, which leads us to believe that security awareness around mobile apps should be increased.

REFERENCES

Canalys. (2011). Smart phones overtake client PCs in 2011. Retrieved 6/11/2016 from http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011
Compomizzi, J. (2013). The influence of iPad technology on the academic and social experiences of veteran and military students: Academic preparation, collaboration socialization, and information access. ROBERT MORRIS UNIVERSITY.

Compomizzi, J., D'Aurora, S., & Rota, D. P. (2013). Identity theft and preventive measures: the cost is all yours. *Issues in Information Systems, 14*(1), pp. 162-168.

Koved, L., Trewin, S., Swart, C., Singh, K., Cheng, P. C., & Chari, S. (2013, July). Perceived security risks in mobile interaction. In Symposium on Usable Privacy and Security (SOUPS).

Petsas, T., Papadogiannakis, A., Polychronakis, M., Markatos, E. P., & Karagiannis, T. (2013, October). Rise of the planet of the apps: A systematic study of the mobile app ecosystem. In Proceedings of the *2013 Conference on Internet Measurement Conference*, pp. 277-290. ACM.

Salesforce. (2014). Mobile Behavior Report. Retrieved 6/9/2016 from http://www.marketingcloud.com/resource-center/digital-marketing/2014-mobile-behavior-report

Statistica, (2016). The Statistics Portal. Number of free and mobile app store downloads worldwide from 2011 to 2017 (in billions). Retrieved from www. Statistica.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A risk assessment method for smartphones. *Information Security and Privacy Research*, pp. 443-456. Springer Berlin Heidelberg.

Tongaonkar, A., Dai, S., Nucci, A., & Song, D. (2013, March). Understanding mobile app usage patterns using in-app advertisements. *Passive and Active Measurement,* pp. 63-72. Springer Berlin Heidelberg.