Journal of International Technology and Information Management

Volume 24 | Issue 4 Article 3

2015

Mobile App Installation: the Role of Precautions and Desensitization

Mark A. Harris
University of South Carolina

Amita Goyal Chin
Virginia Commonwealth University

Robert Brookshire
University of South Carolina

Recommended Citation

Harris, Mark A.; Chin, Amita Goyal; and Brookshire, Robert (2015) "Mobile App Installation: the Role of Precautions and Desensitization," *Journal of International Technology and Information Management*: Vol. 24: Iss. 4, Article 3.
Available at: http://scholarworks.lib.csusb.edu/jitim/vol24/iss4/3

Mobile App Installation: the Role of Precautions and Desensitization

Mark A. Harris
Integrated Information Technology
University of South Carolina

Amita Goyal Chin
Department of Information Systems
Virginia Commonwealth University
USA

Robert Brookshire
Integrated Information Technology
University of South Carolina

ABSTRACT

The purpose of this research is to investigate precautions that consumers take before installing mobile apps and consumer's potential desensitization to excessive app permission requests. Through a survey of 209 participants, a prediction model was created that attempts to predict whether respondents would download applications asking for excessive permissions. The model results indicate those that take more precautions are less likely to download apps requesting excessive permissions. However, the precautions taken by participants may be inadequate and may leave consumers with a false since of security. Another key finding with the support of Communication Theory and the C-HIP Model is that some consumers have become desensitized to excessive permission requests. These consumers knowingly install apps requesting excessive permissions for reasons such as nothing bad has happened to them before, they trust the market, or they really want the app. The security implications of permission desensitization and inadequate precautions are discussed.

Keywords: Mobile APPs, installation of mobile APPs, consumer desensitization

INTRODUCTION

Smartphones and tablets have been rapidly increasing in worldwide sales over the last few years. Gartner predicts smartphones will account for 90% of all mobile phones by 2018 (Gartner, 2014) and tablet sales will surpass PC sales in 2016 (Gartner, 2015). As of fall 2015, Google's Android operating system was on 64% of the world's smartphones and tablets and Apple's iOS was on 23% (Statcounter, 2015). These two platforms lead the mobile market by a larger margin.

The app markets associated with these two popular platforms are Google's Google Play market and Apple's App Store, with each containing over 1.5 million downloadable applications (Statista, 2015). A significant risk to consumers that download and install mobile applications is malware. McAfee (2015) reports that malware is on the rise, with over 1 million new mobile malware samples detected in early 2015. Also, 99% of all mobile malware is written for the Android operating system (Cisco, 2014). However, Apple applications are not without risk. In a report on poplar apps, iOS apps were found to be more risky than Android apps (Appthority, 2014). In addition, the report highlighted that 95% of the top free Android and iOS apps and 80% of paid apps exhibited at least one risky behavior.

With the increase in smart devices, apps, and malware, consumers should take precautions before installing apps. According to research and government agencies, potential precautions consumers can take are to review the app developers (IC3, 2012), use only trusted app markets (FCC, 2014), and read app permissions (Harris et al., 2014). App permission requests are apps asking the consumer for permission to access data or services on the device, such as an app asking to know the consumer's location. Excessive permission requests are apps asking for access to data or services that are not necessary for the app to reasonably function, such as a card game requesting permission to send text messages. Consumers that choose to ignore excessive permission requests and install the app anyway may have become desensitized to excessive permission requests. Two potential reasons for desensitization are that the consumer trusts the market to protect them and nothing bad has happened to them before. Also used as a precaution, but not recommended by researchers, is reading app reviews and star ratings (Kelley et al., 2012)

The purpose of this research is to investigate precautions that consumers take before installing mobile apps and consumer's potential desensitization to excessive app permission requests. Knowing what precautions consumers take before installing apps will be helpful in determining if consumers are taking the proper security precautions. Investigating desensitization to excessive permission requests will be helpful in determining the overall effectiveness of the permission request warning. Consumers may be exposing themselves to increased risk by not fully understanding the proper precautions to take and the risks associated with desensitization.

In the next section, we discuss various precautions that consumers may take when downloading mobile applications. Within this context, we incorporate findings from the research literature and develop our hypotheses. Similarly, we discuss the notion of desensitization, report previous findings, and develop our associated hypotheses. In the next section, we provide a detailed description of our survey instrument, which includes a prediction model for installing applications with excessive permissions. In the final two sections, we offer a discussion of our findings and our conclusions.

Precautions

In this study, we investigate several actions consumers perceive as precautions they may take before downloading and installing a mobile application. One is to review and understand the permission requests, as recommended by researchers and government agencies (FCC, 2014; Harris et al., 2014; IC3, 2012). While other platforms also use permissions, permission requests are more prevalent on the Android platform. Every time a consumer downloads and begins installing an application, a list of permissions needed by the application are displayed for the consumer's consent. This list of permissions tells the consumer what services or data the app needs to function. However, it is important for the consumer to match each permission request with an actual feature of the app. For example, if an app asks for GPS location, what feature in the app would use location? If it is a map app, then that makes sense. If it is a solitaire card game, then asking for GPS location is excessive and not warranted. Consumers should also read the app's description, as some developers explain their permission requests. Carefully reading app permissions is important and research has shown that popular applications, free applications, and mature content applications request more permissions than average (Chia et al., 2012). While permissions are displayed as a warning to consumers, research has shown using app permissions as a precaution has not been an effective security measure because many consumers simply do not read them (Felt et al. 2012; Mylonas et al., 2013) or do not understand them (Benton et al., 2013; Kelley et al., 2012). Based on this previous research, we propose the following hypothesis:

H1: Most consumers will not read app permissions as a precaution before installing a mobile app.

Another action consumers often take as a security precaution is to only install apps from trusted sources, as suggested by researchers and government agencies (FCC, 2014; Harris et al., 2014; IC3, 2012). While malware can be found on traditional markets, like Google's Google Play and Apple's App Store, most malware is found on 3rd party markets (Juniper, 2013). For Android users, accessing 3rd party markets is as easy as checking a security setting in the system settings. This freedom Android gives their users is one of the reasons why malware is more prevalent on the Android platform. Apple users must jailbreak their devices in order to access 3rd party markets, which is a much more difficult process and one reason why Apple's iOS platform is considered safer than Android. When it comes to trusting traditional markets, research suggests that most consumers trust the official markets associated with their platform to deliver safe applications (Kelley et al., 2012; Mylonas et al., 2013; Jones & Chin, 2015; Jones et al., 2014). Therefore, we propose the following hypotheses:

H2: Consumers will trust the major platform markets more than 3rd party markets.

H3: Most consumers will only download apps from trusted markets.

Using star ratings and reading reviews are other actions some consumers take to gauge security of the app. In one study, participants relied heavily on star ratings, full text reviews, and even word of mouth because they were better understood and trusted than permissions (Kelley et al., 2012). However, research has not shown these actions as reliable security methods, such as a study that concluded that community ratings used in app markets are not reliable indicators of app risks and ratings are based on functional aspects like features and performance rather than risks (Chia et al., 2012). Accordingly, we propose the following hypothesis:

H4: Most consumers will use star ratings and reviews as a precaution before installing an app.

Finally, it is recommended that consumers investigate and read reviews about the developers themselves (IC3, 2012; Harris & Patten, 2014). However, no research could be found that investigated developer reviews with the riskiness of the apps they develop. Because research has shown many consumers do not read permission requests, we believe many consumers will also not research the developer. Therefore, we propose the following hypothesis:

H5: Most consumers will not review developers as a precaution before installing an app.

In other permission research, some have suggested unique ways of understanding permission requests. Sarma et al. (2012) suggest a model that compares the app's permission requests to similar apps within the same category, such as an arcade game's app permission requests compared to other arcade game's permission requests. An app asking for more permissions than what is normal for the category may be an indicator of risk. In similar research that investigated permission requests, Bartel et al. (2012) described an approach that analyzed each permission request to see if the app itself had a use for each permission. Permission requests that had no use within the app were seen as permission gaps that could lead to increased security risks. However, the author's approach did not account for permissions that did have functions within the app, but could also be used for malicious intent. For example, an app could have a request to make phone calls and the app may have a technical support number link for that use, but the permission could also be used to call premium numbers without the user's knowledge. This would be considered an excessive permission request if the feature was beyond a reasonable expectation for the type of app.

Other research suggests a new permission interface that does a better job of explaining the privacy concerns of requested permissions (Kelly et al., 2013). That authors proposed and tested a new GUI interface that read the requested permissions and displayed the privacy concerns to the user in a much more easy to read format.

Desensitization

In this paper, desensitization refers to consumers being numb to permission requests, particularly excessive permission requests, and installing the app anyway. Apps designed for Android versions older than 6.0 will display dangerous permission requests at the time of installation as a warning to consumers. Apps designed for version 6 and later and run on a version 6 or later operating system will display permission requests after installation and when the app needs the specific permission.

Warning effectiveness and desensitization has been researched in multiple fields, such as product and workplace warnings (Schwartz & Driver, 1983), tornado warnings (Simmons & Sutter, 2009), flood warnings (Molinari & Handmer, 2011), cigarette label warnings (Hammond et al., 2006), and computer security warnings (Krol et al., 2012; Akhawe & Felt, 2013). However, only one study investigated desensitization of app permission requests (Harris et al., 2016). In their study, desensitization was investigated as an antecedent to trust and risk in relation to the intent to install apps. The authors concluded that desensitization was not a significant factor, but it did have a negative relationship with risk and a positive relationship with trust, meaning that those that are desensitized perceive less risk and more trust.

In technology-related warning and desensitization research, Krol et al. (2012) investigated users receiving a warning before downloading a PDF file. The authors found that 81.7% of the participants did not heed the warning and downloaded the file. A reason for ignoring the warning was that users had become desensitized to frequent exposure to warnings and false alarms. Users also had misunderstandings about the potential security threats which led them to falsely believe they could recognize the security risks. The study also found that those that heeded the warnings were overwhelmingly female. Based on this finding, we created the following hypothesis:

H6: A higher percentage of females will resist installing apps with excessive permission requests than males.

In a study that investigated certificate warnings when entering Web sites, Kauer et al. (2012) found that a majority of participants did not understand the warnings. Also, of those that chose to enter the site despite the warning, the primary reason given was that they trusted the site. Others stated that they perceived no risk because nothing bad had happened to them before. Based on the findings in this study, we propose the following hypothesis:

H7: Of those that install apps with excessive permission requests, most will do so because they trust the market.

A possible explanation for desensitization to warnings can come from Communication Theory. In a paper that discussed using Communication Theory for creating product warnings and warnings in the workplace, Schwartz and Driver (1983) discussed comprehensive warnings versus selective warnings. Comprehensive warnings attempt to display all potential hazards in great detail. Selective warnings display only a limited number of select hazards. The author's discussion on these types of warnings lead to several interesting aspects that may help explain desensitization. One is that when too much information is given, comprehension of the message may suffer. Consumers have a limited ability to absorb information and giving too much information may discourage consumers from even attempting to address the warning (Schwartz & Driver, 1983). Another is that if the consumer perceives one of the hazards in the warning as a minimal concern, they may discount the importance of the other hazards addressed in the warning. Also, if consumers receive a significant number of comprehensive warnings across multiple products, then all product warnings become less effective. Over-warning can lesson warning credibility. Consumers installing many apps will likely see permission request warnings with each app. Some apps may have long lists of permissions seen as comprehensive warnings by consumers and some may have warnings seen as minimal risks by the consumer. Desensitization to permission requests may occur under these conditions.

The Communication-Human Information Processing (C-HIP) Model was developed using pieces of Communication Theory. The C-HIP Model has several stages, one of which is "beliefs and attitudes." In a paper by Conzola and Wogalter (2001), the authors explain that a warning can be processed successfully if it matches the receiver's current beliefs and attitudes. However, when people believe they are familiar with a product, they are less likely to read the warnings even if they see them (Conzola & Wogalter, 2001). Familiarity beliefs are formed from similar past experiences and can lead to complacency and overconfidence and reduces the likelihood a consumer will seek additional information, thus reducing the likelihood of reading warnings (Conzola and Wogalter, 2001). Consumers that install many apps become familiar with the process of using markets and installing apps. This familiarity may lead consumers to ignoring permission requests.

In other research about desensitization to warnings, Stewart and Martin (1994) discuss two types of false alarms. One is a genuine warning false alarm in which a warning proves incorrect because nothing was at risk. The other is an apparent warning false alarm, in which risk is present, but no immediate harm follows from a failure to heed the warning (Stewart & Martin, 1994). An apparent false alarm is not actually false, but consumers may treat warnings as false alarms when they cannot connect the warning with an immediate consequence. Consumers become desensitized to the warnings after repeatedly ignoring the warnings and suffering no immediate consequences (Stewart & Martin, 1994). When it comes to permission request warnings, consumers may be desensitized because they cannot make a direct connection with the requests and an immediate harm. Consumers may see permission requests as apparent false alarms. Based on this research and the C-HIP Model, the following hypothesis is proposed:

> **H8: Of those that install apps with excessive permission requests, a majority will do so because nothing bad has happened to them before.**

Survey

To assess precautions taken by consumers before installing mobile applications and desensitization to permission requests, a 34 question online survey was given via Qualtrics in late 2014 and early 2015. A total of 286 surveys were sent to students registered for information technology classes, which included IT majors and minors. Of those sent, 227 (79%) were returned and 209 (73%) were complete for analysis. Respondent's ages ranged from 17 to 55, with a mean of 23.33. One hundred sixty-two (77.5%) were male and 47 (22.5%) were female. One hundred seventy (81%) of the respondents were or had been technology majors, studying information technology or computer science.

ANALYSIS AND RESULTS

The respondents were asked to specify the operating system on their primary smartphone, tablet, or both. More respondents used Apple's iOS, 60.8%, than did Google's Android, 43.5%. A small percentage of respondents, 4.3%, reported using both iOS and Android. Beyond Google and Apple, 3.3% reported using other operating systems. Respondents were asked to report the number of unique applications they had downloaded on their current device, with a result mean of 34. Respondents were asked whether they had rooted or jailbroken their device, and 19.7% responded affirmatively, while 76.5% said they did not have such a device and 3.8% of respondents did not know. There was no association between having a rooted device and the operating system used, nor was there an association with the user's gender.

Slightly fewer than half, 48%, of respondents reported having been a victim of malware and 52% saying they had not been victims. Once again, there was no association with being a victim of malware and the operating system used or the respondent's gender. However, those with rooted devices were more likely to be victims of malware (chi square=6.772, df=1, p=0.034).

Market Trust

We asked respondents to rate their trust in Google's Google Play market, Apple's App Store, Amazon's App Store, Microsoft's App Store, and other 3rd party markets. In this study, the primary markets are seen as those from Google, Apple, Microsoft, and Amazon. Amazon is included because of its size, popularity, and reputation for security. All others are seen as 3rd party markets. The participants rated the markets in five different areas: protecting their personal information, such as credit card data; charging the correct amount for an application; limiting applications from asking for excessive permissions; selling applications that perform as advertised; and protection from malware. The ratings were on a five-point scale, with 1 indicating "Not Trustworthy" and 5 indicating "Very Trustworthy." We then summed these evaluations to get an overall trust score for each market, ranging from 5 to 25.

In general, the primary markets evaluated similarly. The Apple and Google markets had average trust ratings of 17.42 and 16.96, respectively. The Amazon market had an average rating of 16.76, while the Microsoft market's average rating was 16.0. Third party markets received an average trust rating of 12.91. Multivariate tests (F=66.545, df=4,205 p<0.001) show that the Apple, Amazon, and Google markets were trusted significantly more than the Microsoft market (p<0.001, p=0.002, and p=0.022, respectively). This may be because very few participants used the Microsoft market and unfamiliarity led to less trust. Third party markets were significantly less trusted than all the others (p<0.001 for all paired comparisons). Therefore, H2 is supported.

H2: Consumers will trust the major platform markets more than 3rd party markets. (SUPPO RTED)

Also, users of Apple's iOS operating system evaluated third-party markets slightly higher than non-iOS users (t=2.015, df=207, p=0.045). This may be because Apple restricts users from accessing 3rd party markets and Apple users may not as aware of the risks associated with 3rd party markets. In addition, Android users evaluated the Apple market lower than non-Android users (t=-2.758, df=207, p=0.006). We know from the market trust results that Apple users trust their primary market more than Android users trust their primary market, so perhaps Android users carry over that lower level of trust when evaluating the Apple market. Lastly, Android users evaluated third party markets lower than non-Android users (t=-2.842, df=207, p=0.005). Again, this may be explained by Android users generally being less trusting of markets.

Of our 209 participants, 94.7% only downloaded their apps from trusted markets, which in this study includes Apple's App Store, Google's Google Play, Windows Phone App Store, and Amazon's App Store. Only 5.3% of respondents used 3rd party markets outside of these trusted primary markets. When investigating just Android users, which is an easier platform for accessing 3rd party markets, only 6.6% did so. These findings support H3.

H3: Most consumers will only download apps from trusted markets. (SUPPORTED)

Precautions

We asked survey respondents about the precautions they took before installing applications, including whether they read the reviews/star ratings of applications, if they investigate the application's developers, whether they read the permissions requested by the application, or whether they take other precautions. Eighty-three percent said they read the application's reviews/star ratings as a precaution, which supports H4. Fifty-five percent said they read the requested permissions, which does not support H1, but is close to supporting it. This means 45% do not read permissions as a precaution. Only 26% said they investigated the application's developer, which supports H5. Three percent said they take other precautions, including "common sense," "reading tech blogs," "reading the source code," and "checking the number of downloads."

H1: Most consumers will not read app permissions as a precaution before installing an app. (NOT SUPPORTED)

H4: Most consumers will use star ratings and reviews as a precaution before installing an app. (SUPPORTED)

H5: Most consumers will not review developers as a precaution before installing an app. (SUPPORTED)

We counted the number of precautions each respondent took. Twelve percent took no precautions at all, while 30% took only one precaution. Thirty-eight percent said they took two precautions, while 19% took three precautions. There was no association between the number of precautions taken and whether the respondent had a rooted device or was a victim of malware. Apple iOS users were more likely than non-iOS users to take no precautions at all, with 17% taking no precautions (chi square=103.415, df=3, p=0.004, Somer's d=-.255). Android users were slightly more likely to take more precautions (chi square=25.503, df=3, p<0.001, Somer's d=0.372). This may be because iOS is considered a safer platform than Android.

Desensitization

We asked survey respondents if they were likely to abort the installation of an application that asked for excessive permissions, such as asking to access their contacts or track their locations. Seventy-seven percent of respondents said that they agreed or strongly agreed that they would abort the installation of this kind of application, while only 10% of respondents disagreed or strongly disagreed.

Investigating intent, we then asked respondents under what circumstances they would ignore an application asking for excessive permissions and install it anyway. Table 1 shows their responses to several scenarios they were presented. The circumstances under which a majority of respondents said they would ignore permission requests were if they trusted the market, nothing bad has happened to them before, and if they really wanted the application. They were less likely to ignore the permission requests if whenever they read the permissions, everything looked OK, if they did not understand the requests, or if it took too long to read the requests. As Table 1 shows, however, sizeable minorities of respondents would ignore permission requests under these circumstances.

Table 1: Circumstances under Which Respondents Ignore Excessive Permission Requests and Install the App Anyway.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total
I trust the market.	7 (3.3%)	38 (18.2%)	44 (21.1%)	97 (46.4%)	23 (11%)	209
Nothing bad has happened to me before.	14 (6.7%)	50 (23.9%)	38 (18.2%)	92 (44%)	15 (7.2%)	209
I do not understand the permission requests.	26 (12.4%)	75 (35.9%)	55 (26.3%)	44 (21.1%)	9 (4.3%)	209
It takes too long to read them.	24 (11.5%)	53 (25.4%)	47 (22.5%)	69 (33%)	16 (7.7%)	209
Whenever I read them, the always look OK.	12 (5.7%)	40 (19.1%)	70 (33.5%)	72 (34.4%)	15 (7.2%)	209
I really want the application.	14 (6.7%)	38 (18.2%)	53 (25.4%)	86 (41.1%)	18 (8.6%)	209

We asked survey respondents if they had ever actually installed an application that they believed asked for excessive permissions. Fifty-six percent said they had installed such applications anyway, while 44% said they had not. There was no association between installing these applications and whether the respondent had a rooted device, was a victim of malware, was an iOS user, or was an Android user. Forty-five percent of the female respondents had installed apps asking for excessive permissions and 59% of the male respondents had done so. This supports H6.

H6: A higher percentage of females will resist installing apps with excessive permission requests than males. (SUPPORTED)

For those respondents who had installed applications asking for excessive permissions, we asked further questions to see what would prompt them to do so. Of the 116 who installed such applications, 68% said they did so because they trusted the market from which they downloaded the application. This supports H7.

H7: Of those that install apps with excessive permission requests, most will do so because they trust the market. (SUPPORTED)

Fifty-eight percent said there was often a good reason for the application to request the permissions. Another 54% said they just wanted the application and did not care about the permission requests, while 53% said that nothing bad had happened to them when they had installed such applications before. This supports H9.

H8: Of those that install apps with excessive permission requests, most will do so because nothing bad has happened to them before. (SUPPORTED)

Prediction Model

In an effort to predict the behavior of survey respondents with excessive permission requests, we constructed a prediction model designed to predict whether respondents would install applications asking for excessive permissions (0=yes, 1=no). A logistic regression model was used to estimate the model with this as the dependent variable. Independent variables entered in the preliminary model were the evaluations of the five markets, whether the respondent used iOS, the respondent's age and gender, the number of precautions taken, and whether the respondent was a technology major.

Using stepwise entry of the independent variables based on the likelihood ratio criterion, a model including only the number of precautions was significant. Table 2 shows the model statistics. In logistic regression, the Hosmer and Lemeshow chi square statistic is used to test the hypothesis that the predicted values are significantly different from the observed values (Hosmer & Lemeshow, 2000). The Hosmer and Lemeshow test indicated that there was no significant lack of fit between the model and the data (chi square=0.657, df=2, p=0.720). The Nagelkerke R2 value was developed to show the amount of variation accounted for by a logistic regression model. As with a linear regression, values range between 0 and 1, with 1 indicating a perfect fit (Hair, et al., 2006). The Nagelkerke R^2 value was 0.044. The model shows those who take more precautions are somewhat less likely to download applications with excessive permission requests than those who take fewer precautions. The security savviness of these users is better in that they take increased precautions and avoid apps asking for excessive permissions.

Table 2: Prediction Model Logistic Regression Model.

Variable	B	Standard Error	Significance	Exp (B)
Constant	.437	0.287	0.128	1.548
# of Precautions	-0.405	0.155	0.009	.667

The exponentiated regression coefficient value is .667. This indicates that each additional precaution a respondent takes reduces the odds that he or she will install an app asking for excessive permissions by one-third.

Table 3 shows the predictive accuracy of the model. As shown in the table, the model classified 59.8% of the respondents correctly, with better success in the Yes condition (65.5%).

Table 3: Prediction Model Logistic Model Accuracy.

		Predicted		
		Have you ever installed an application you believed asked for excessive permissions?		Percentage Correct
Observed		Yes	No	
Have you ever installed an application you believed asked for excessive permissions?	Yes	76	40	65.5
	No	44	49	52.7
Overall Percentage				59.8

DISCUSSION

Participants in this study averaged over 34 downloads each, which establishes the sample as a group that has significant experience with mobile applications. Unlike worldwide and national averages, this group had more iOS representation than Android representation. Almost one in five of those surveyed rooted or jailbroke their devices, which made them more likely to be a victim of malware in this study. Rooting or jailbreaking a mobile device removes the built-in security restrictions, making the devices more vulnerable to malware. Thus, this result is expected and fits current research trends.

Participants in the study trusted the Apple App Store and the Google's Google Play markets significantly more than Microsoft's market, which was a little surprising considering Microsoft is a major market with their own platform. However, all three of these markets and Amazon are seen as significantly more trustworthy than 3rd party markets, which fits current research that suggests most malware is present on 3rd party markets.

More than half of those surveyed installed apps asking for excessive permissions. However, installing apps asking for excessive permission must come with major concerns based on the survey results indicating 84% agree or strongly agree that they are very concerned with protecting their privacy and 78% agree or strongly agree that they are concerned with malware. There appears to be contradiction with one's concern for privacy and malware and the installation of apps asking for excessive permissions.

Of those who installed apps with excessive permissions, 68% said it was because they trusted the market. However, all markets contain malware, ask for excessive permissions, and have major privacy concerns (Harris et al., 2014). The before mentioned Appthority (2014) study indicated that Apple's App Store's top apps were more risky than Google Play's top apps and our survey participants trusted the Apple App Store the most. With 58% stating there is often a good reason for the application to request questionable permissions and 53% stating nothing bad had happened to them before, there is an indication of desensitization among consumers. This supports theoretical research using Communication Theory and the C-HIP Model. When consumers no longer reject apps with excessive permissions because nothing has ever happened to them before and the belief that there is a good reason for the permission requests if they were to investigate, those consumers have become desensitized to excessive permission requests. Desensitization to permission requests puts the consumer at great risk and renders permission request lists even more inadequate. Consumer desensitization to excessive permission requests is also supported by the before mentioned (Benton et al. 2013) study that concluded permissions were still ineffective even after adding additional text warnings to permission requests.

A prediction model was presented in this paper that attempts to predict whether participants will download applications asking for excessive permissions. Research demonstrates it is highly advisable to avoid apps with excessive permissions (Harris et al., 2015). Those that took more precautions installed less apps with excessive permission requests. While this may indicate sound security behavior by taking more precautions and downloading less apps with excessive permissions, avoiding apps with excessive permissions is the more important security practice. This is because while taking more precautions may seem like a good thing, the particular precautions taken by our participants are not all sound security precautions. For example, this paper has already established that application star ratings and reviews are not related to security risk, thus are not adequate as a security precaution. Reviewing the developer can be a good security precaution, but it is not efficient because there are many developers with little or no information available about them. Unless there is published negative information about a developer, it is hard to determine a developer’s credibility. Also, if a developer has published negative information, they may be less likely to have apps on the major markets to begin with. Thus, only developers with clean records will have apps on the major markets, making it harder to research developers. Only 26% of the participants in this study reviewed the developer as a precaution. The best precaution these consumers can take is to thoroughly review and understand the app permissions and how they affect security. However, this paper has already established that users most often fail to understand permission requests even if they read them. In addition, those that do understand the permission may be desensitized to them. Overall, the precautions our participants are taking are mostly ineffective and may be giving consumers a false sense of security, thus leading to the highly reported victimization from malware (48%).

The results of this study have implications for businesses that should be a major concern. With the popularity of BYOD, businesses need to be aware of employee’s mobile device security practices. If devices are used for both business and personal use, whether business issued or BYOD, apps that can access the devices contacts, phone numbers, phone ID, location, text messages, and more may gain access to sensitive business data. Devices used for business and personal use is a relatively new phenomena that businesses are still learning how to address. Large organizations with highly skilled information technology security teams have begun to address the issue with enterprise mobile management systems (EMMs), mobile device management systems (MDMs), enterprise app markets, and other technologies. However, smaller businesses with limited resources that are not utilizing these technologies are at more risk. All organizations need to be aware of their employee’s potential problematic mobile device security practices and address those concerns through awareness and education programs. But organizations with limited information security technologies need to be even more vigilant at educating their employees about the risks associated with mobile apps, permission requests, and desensitization.

CONCLUSION

This study investigated the influences on consumers before downloading and installing mobile applications. A prediction model was created, and the study results indicate that increased efforts to educate consumers about potential security and privacy risks from permission requests and desensitization are necessary. Additionally, efforts are needed to inform consumers about the unreliability of common precautions, such as researching developers and app reviews\star ratings. New methods that simply explain permission requests may not suffice if consumers have become desensitized.

This paper contributes to the existing research literature in several important ways. First, the current study develops and presents a unique model to help predict the installation of apps asking for excessive permissions. Second, the results of the current study delineate the need for changing the way permissions are displayed and explained to consumers, for this may largely be ineffective, particularly if consumers have become desensitized to app permission requests. Finally, the current study contributes to the existing knowledge base in that it clearly demonstrates that consumers still do not understand what precautions should be taken before installing apps. There is too much reliance on reviews and star ratings and not enough reliance on reading, comprehending, and heeding permission request warnings.

As with all studies, this study has some limitations. First, since the sample population surveyed consisted largely of information technology students, and all of these students were from the same educational institution, generalizability of the results may be limited. A future research direction is to diversify the demographics of the population to students from a variety of majors. In addition, surveying students in different institutions across different regions would enrich the data collection. Another extension of this research is to survey professionals and compare the results from this data to that of the student population. Analyzing results from such a larger data set may highlight trends that would be more generalizable.

REFERENCES

Akhawe, D., & Felt, A. P. (2013). Alice in Warningland: A large-scale field study of browser security warning effectiveness. In *Usenix Security*, 257-272.

Appthority. (2014). App Reputation Report https://www.appthority.com/learn/ (Accessed 10 March 2015).

Bartel, A., Klein, J., Le Traon, Y., & Monperrus, M. (2013). Automatically Securing Permission-Based Software by Reducing the Attack Surface: An Application to Android. *arXiv*, 1206.5829v2 [cs.CR] http://arxiv.org/abs/1206.5829 (Accessed 14 November 2015).

Benton, K., Camp, L. J., & Garg, V. (2013). Studying the effectiveness of android application permissions requests. *Fifth International Workshop on Security and Social Networking 2013*: San Diego, CA.

Chia, P., Yamamoto, Y., & Asokan, N. (2012). Is this App safe? A large scale study on application permissions and risk signals. *International World Wide Web Conference Committee*: Lyon, France.

Cisco. (2014). Cisco 2014 Annual Security Report. http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html (Accessed 10 March 2015).

Conzola, V., & Wogalter, M. (2001). A Communication-Human Information Processing (C-HIP) approach to warning effectiveness in the workplace. *Journal of Risk Research,* 4(4), 309-322.

FCC (2014). Ten Steps to Smartphone Security for Android. http://www.fcc.gov/smartphone-security/Android (Accessed 10 March 2015).

Felt, A., Hay, E., Egelman, S., Haneyy, A., Chin, E., & Wagner, D. (2012). Android Permissions: User Attention, Comprehension, and Behavior. *Symposium on Usable Privacy and Security 2012*, Washington, DC, USA.

FTC (2014). Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent. https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million (Accessed 10 March 2015).

Gartner (2014). Gartner Says Sales of Smartphones Grew 20 Percent in Third Quarter of 2014. http://www.gartner.com/newsroom/id/2944819 (Accessed 10 March 2015).

Gartner (2015). Gartner Says Tablet Sales Continue to Be Slow in 2015. http://www.gartner.com/newsroom/id/2954317 (Accessed 10 March 2015).

Hammond, D., Fong, G. T., McNeill, A., Borland, R., & Cummings, K. M. (2006). Effectiveness of cigarette warning labels in informing smokers about the risks of smoking: findings from the International Tobacco Control (ITC) Four Country Survey. *Tobacco Control*, 15(3).

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Latham, R. L. (2006). Multivariate Data Analysis, 6th ed. Upper Saddle River, NJ: Pearson Prentice Hall.

Harris, M. A., & Patten, K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22(1), 97-114.

Harris, Mark A., Furnell, S., & Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy & Security,* 10(4), 186-202.

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

Harris, M. A., Brookshire, R., Patten, K., & Regan, B. (2015). Mobile application installation influences: have mobile device users become desensitized to excessive permission requests? *Proceedings of the Twentieth Americas Conference on Information Systems (AMCIS 2015),* Fajardo, Puerto Rico, August 13-15.

Hosmer, D. W., & Lemeshow, S. (2000). Applied Logistic Regression, 2nd ed. New York: Wiley.

IC3 (2012). Smartphone users should be aware of malware targeting mobile devices and safety measures to help avoid compromise" http://www.ic3.gov/media/2012/121012.aspx (Accessed 10 March 2015).

Jones, B., & 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*, 35(5), 561-571, http://dx.doi.org/10.1016/j.ijinfomgt.2015.06.003.

Jones, B., Chin, A., & Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends, 58*(6), 73-83.

Juniper (2013). Juniper Networks Third Annual Mobile Threats Report. http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf (Accessed 10 March 2015).

Kauer, M., Pfeiffer, T., Volkamer, M., Theuerling, H., & Bruder, R. (2012). It is not about the design – it is about the content! Making warnings more efficient by communicating risks appropriately. *GI-Edition - Lecture Notes in Informatics*, Sicherheit.

Kelley, P., Consolvo, S., Cranor, L., Jung, J., Sadeh, N., & Wetherall, D. (2012). A conundrum of permissions: installing applications on an android smartphone. FC 2012 Workshops, Springer2012.

Kelley, P., Cranor, L., & Sadeh, N. (2013). Privacy as Part of the App Decision-Making Process. *CHI Conference on Human Factors in Computing Systems.* Paris, France — April 27 - May 02, 2013.

Krol, K., Moroz, M., & Sasse, M. (2012). Don't work. Can't work? Why it's time to rethink security warnings. *7th International Conference on Risk and Security of Internet and Systems (CRiSIS),* IEEE, Ireland, October 10-12.

McAfee (2015). McAfee Labs Threats Report, May 2015. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf (Accessed 25 August 2015).

Molinari, D., & Handmer, J. (2011). A behavioural model for quantifying flood warning effectiveness. *Journal of Flood Risk Management*, 4(1), 23-32.

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

Sarma, B., Li, N., Gates, C., Poltharaju, R., & Nita-Rotaru, C. (2012). Android Permissions: A Perspective Combining Risks and Benefits. *Symposium on Access control Models and Technologies (SACMAT),* June 20–22, 2012, Newark, New Jersey, USA.

Schwartz, V. E., & Driver, R. W. (1983). Warnings in the workplace: The need for a synthesis of law and communication theory. *University of Cincinnati Law Review*, 52(38).

Simmons, K., & Sutter, D. (2009). False alarms, tornado warnings, and tornado casualties. *Weather, Climate, and Society*, 1, 38-53.

Statcounter (2015). Statcounter Global Stats. http://gs.statcounter.com/#mobile+tablet-os-ww-monthly-201410-201510 (Accessed 12 November 2015).

StatCounter (2015). Top 8 Mobile Operating Systems from July 2014 to July 2015. http://gs.statcounter.com/#mobile_os-ww-monthly-201407-201507 (Accessed 25 August 2015)

Statista (2015). Number of Apps Available in Leading App Stores as of July 2015. http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ (Accessed 25 August 2015)

Stewart, D., & Martin, I. (1994). Intended and unintended consequences of warning messages: a review and synthesis of empirical research. *Journal of Public Policy & Marketing,* 13(1), 1-19.