www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 09 September 2016 Page No.18210-18216

Risk Perception And Behavior Using In Mobile Security

Dr.M.Sornamageswari[1], C.Bathma[2]

[1]assistant Professor, Cs Department, Government Arts College, Coimbatore, Tamilnadu, India
[2]m.Phil Scholar, Cs Department, Government Artscollege, Coimbatore, Tamilnadu, India
e-mail: bathma60@gmail.com

Abstract— *Security has long been a technical problem with technical solutions. Over time, it has become apparent that human behaviour is a major weakness in technical solutions. Extensive efforts have been taken to inform individuals about the threats and safeguards with which to protect against such threats. Organizations have developed awareness campaigns to enhance the security of employees. These awareness campaigns seek to provide employees with information about a threat as well as measures to take to prevent against the threats. This dissertation investigates the effectiveness of various security awareness message themes as well as the individual perceptions and characteristics that affect security behaviour. First, a survey study is conducted which measures perceptions surrounding security threats and safeguards. The analysis of the survey data builds a foundational understanding of how individuals assess and respond to technical security threats. Next, via awareness themes are evaluated through the use of targeted interventions with non-complying individuals presented awareness messages. The individual responses to interventions and surveys allow for the usage of personality data to inform both initial security safeguard behaviour as well as response behaviour to targeted awareness messages. Overall, the tested awareness methods were found to be somewhat effective. However, with the addition of individual information, analysis identified correlations with individual response. These correlations point to the importance of considering individual motivations and perceptions surrounding security threats and safeguards.*

Keywords-Mobile security; P2P; TTAT; Risk Perception.

I. INTRODUCTION

In this perception, we set out to examine how the perception of risk a user has relates to current security . Different behaviours could have drastically different perceptions which could result in different behaviours regarding safeguard usage. For example, locking a Smartphone and installing antivirus on a Smartphone are different behaviours on multiple levels. First, screen locking protects against a physical threat where antivirus software focuses on a remote, software based threat. Second, setting up a screen lock requires a constant interaction from a user every time a device is turned on or accessed. Whereas mobile antivirus software requires the initial e ort of installing an application and is mainly autonomous from that point forward. While a user is able to interact with the antivirus software, there is no significant cost to the user once the antivirus app has been installed. These differences may play a role in the varying perceptions of each behaviour. As mentioned TTAT suggests that behaviour is based on avoidance motivation which is based on a combination of perceptions regarding both the threat and associated safeguards. To explore the differences in perceptions, a survey study was conducted in which risk perceptions were collected on four different threat and safeguard scenarios. In addition to perceptions of risk, data regarding current security behaviours congruent to the presented scenarios was collected. This allowed for the comparison between risk perceptions and actual behaviour. Finally, basic demographic information, familiarity with

technology, and general risk propensity information was collected. With all of this information, an insightful analysis can be conducted which explores the relationships between perceptions and behaviour before awareness messages are presented.

II. CONTRIBUTIONS

Individual risk perceptions vary across behaviours. Survey participants as a whole had lower levels of awareness of the benefits of mobile antivirus and dangers of peer to peer le sharing when compared to awareness levels of mobile screen locks. Interestingly, the cost associated with using mobile antivirus software on a mobile phone was significantly higher than the cost associated with using a screen lock while the levels of inconvenience associated with each safeguard were much more similar. Age is a significant factor in both risk perceptions and security behaviours. The results of the survey study indicate a strong relationship between age and risk perceptions. Specially, older individuals are more likely to have a lower perception of controllability; with three out of the four threat scenarios we studied exhibiting this trend. Additionally, older individuals are more likely to employ security safeguards. There are strong relationships between risk perception and safeguard usage. Data from the survey study supports the Technology Threat Avoidance Theory (TTAT).

Additionally, levels of knowledge and impact are strongly correlated with safeguard usage across all of the threat scenarios. Familiarity with technology correlates strongly with variations in risk perception. Higher levels of familiarity with technology (i.e. Internet, Computers, Social Networks, Mobile devices), measured by frequency of usage, correlate to significant differences in risk perception. Increased familiarity relates to higher levels of perceived knowledge, impact, severity, and awareness of a threat. De-creased levels of familiarity with mobile devices relates to increased levels of perceived controllability. Overall, this chapter presents evidence that initial behaviours are strongly linked to perceptions of both threats and the associated safeguards.

III .THREAT AND SAFEGUARD SCENARIOS

The threat and safeguard scenarios covered in the survey study are summarized in Table 3.1. The first scenario focused on enabling screen locks on mobile devices. Locking behaviour is further investigated in phone locking Second, the usage and perceptions of mobile antivirus are evaluated. Further exploration of mobile antivirus is detailed in mobile antivirus. Third, the threat of downloading infected les through peer to peer le sharing services is covered. Finally, perceptions of threats to social information privacy are explored in the Social Privacy scenario. This scenario addresses the threat of personal information being exposed to unintended parties due to publishing the information on social networks. These behaviours were chosen as it was believed they represent a broad range of behaviours that are somewhat different in nature. Three behaviours, locking a phone, installing antivirus, and checking privacy settings, focus on doing something to pre-vent a threat from occurring. The P2P behaviour focuses on refraining from le sharing activities in order to avoid an infection. Also, the AV scenario represents a less obtrusive safeguard as compared to the Locking safeguard as Locking requires repeated usage and memory of a lock while antivirus software requires a onetime install. Both the AV and Social Privacy scenarios address scenarios that are relatively new and may have a lower level of awareness as compared to the other behaviours.

IV .STUDIED PERCEPTIONS

In the background technology threat avoidance theory suggests that users will try to avoid risks associated with IT related activities. Fiasco was able to contextualize threats by using death but when it comes to Information Security, it is much more difficult to quantify and contextualize risk. Huang .l extended the work by Fiasco and Slavic with a focus on information security. Factors are identified in both of these models and are measured using multiple statements for each factor as outlined in Appendix A. Each of these statements are measured asking participants how much they agree with a

statement using a 7-point Liker scale with (1=Strongly Disagree, 7=Strongly Agree). The statements are then averaged together to make up the overall factor score. Psychometric Paradigm of Risk Perception: The `Knowledge' factor addresses people's knowledge of and familiarity with a given threat. The `Impact' factor is made up of both the scope (how wide ranging the consequences are) and duration (how long consequences last) of impacts associated with the threat. The `Severity' factor is made up of not only severity but also personal exposure and perceived voluntariness of the threat. The 'Controllability' factor addresses how much control a participant feels they have over the threat. That is, to what extent the threat can be prevented, how observable the threat is, and how predictable the threat is. If a person feels they do not have much control over a threat, they may associate a higher risk with such a threat as they feel helpless. The `Possibility' factor address how likely the participant believes it is for the threat to happen to them. Threats that are perceived as more likely may associate with a higher risk than those that may not be as frequent.

Finally, the `Awareness' factor is composed of both immediacy of effect and whether or not the threat is known to those that are exposed to it. That is to say, higher levels of awareness would mean that when a threat occurs, it is likely that people will be aware of it happening. If a virus wipes the hard drive in a computer, it is likely that the users of that computer will be highly aware that something bad happened. In contrast, if a computer happens to become infected with spyware which covertly steals data from the computer without making its presence know, it is not likely that users would be aware that the threat was occurring.

Technology Threat Avoidance Theory: Threat avoidance behaviour is based on users believing a threat is likely to happen to them (Perceived susceptibility) and have severe consequences (Perceived Severity). Once a user believes a threat should be avoided, they will take action to avoid the threat if they believe they are capable of implementing the safeguard (Selfecacy) and that the safeguard is both effective (Perceived Safeguard Effectiveness) and inexpensive (Perceived Safeguard Cost).

Risk Propensity: The survey presents the participants with two risk propensity scales. The risk propensity scales were used to judge the general tendency of an individual to take risks. The scales asked participants several questions regarding behaviours related to risks and avoidance of risks. These scales were based on previously used risk propensity scales [80, 125]. Each of the scales presented participants with six statements regarding risky behaviours and ask participants how much they agree with each of the statements using a 5-point Liker scale. The statements are then averaged together to represent an overall risk propensity score that we label RP1 and RP2 with RP2 representing the more generalized score that focuses less on business than RP1.

V. SURVEY SETUP

This study used an internet-based survey tool to collect responses from self-selected individuals on Amazon's Mechanical Turk (Murk) service. Murk is a marketplace for work [126]. Murk requesters post Human Intelligence Tasks (HITs) and Murk workers select from thousands of tasks and get paid per completed HIT. Research has shown that the Murk population is a diverse population sample that is representative of the U.S. population [127, 128].
down window on the left of the MS Word Formatting toolbar [8,9,10].

The survey was developed using the Qualtrics survey platform [129]. The questions were divided up into seven blocks. First, participants were presented with demographic questions regarding education, employment, and general technology usage questions. The next four blocks presented the participants with four threat/safeguard scenarios. These four blocks were exactly the same except for the described threat scenario and associated safeguard to use to protect against the threat. The questions contained in these blocks consisted of the risk factor questions from Huang et al. [124] and

questions to address the factors from the Technology Threat Avoidance Theory [3]. All of the questions in each of these four blocks were presented in a randomized order and were ranked on a 7-point Linker scale (1=Strongly Disagree, 7=Strongly Agree). The next block asked users about their security behaviours associated with the technology they indicated they used. Users who did not use mobile devices were not presented with questions regarding mobile password or antivirus usage. Finally, the users were presented with the two risk propensity scales.

Amazon Mechanical Turk was used to recruit survey participants. The survey was posted as a HIT indicating it should take about twenty minutes to complete and had a reward of $0:75. The HIT was posted with a limit of 300 participants and was completed in four days. Individual completion times varied by participant with the distribution being shown in Figure 3.1. Based on internal testing, a conscientious survey taker would spend at least 15 minutes completing the survey. The average time to complete the survey was 21.22 minutes. Of the original 300 surveys, 32 of the surveys were completed in under 10 minutes. Therefore, surveys which took less than 10 minutes may not contain serious answers and were altered. The new average time for completion is 22.82 minutes. Additionally, 1 participant submitted two surveys, so the second submission was altered out as well. In the end, 267 survey responses were left in the dataset.

VI.RESULTS

The survey was limited to participants 18 years of age and older with the average age being 37.2 years and the distribution depicted in Figure 3.2. Gender was mostly balanced within the population with females making up 56.9% (152 females, 115 males) of the sample. The majority of the population had completed at least two years of college as shown in Figure 3.3. Figure 3.4 shows the distribution of employment of survey takers with most participants considering themselves “Employed for wages". It should be noted that participants may consider Amazon Mechanical Turk to be their source of income as many people use Murk as a full time job [130].

6.1 Psychometric Factors

Individual perceptions based on the psychometric risk paradigm varied between different threat and safeguard scenarios. Therefore, in this section, analysis will focus on

Differences of perception scores for the same individual across scenarios. Pair wise comparisons were perfumed using paired t-tests and Bonferroni correction to adjust for the family wise error rate. Figure 3.5 shows Knowledge scores and although it appears there are similar average levels of scores, pair wise comparisons identified differences between some behaviour as shown in Table 3.4. AV Knowledge was significantly lower than any of the other behaviours with the largest mean difference being with Locking with a mean difference of: 393 (Paired t-test, p = 3:7e 06, df = 266, t = 5:0735). This indicates that the knowledge of the need for mobile antivirus is significantly less than other the other threat scenarios surveyed.

While the scores for Impact appear to be very similar in Figure 3.6, pair wise comparisons using a paired t-test resulted one pair having significance as identified as shown in Table 3.5. There was a significant difference between Locking and Social Privacy with Locking resulting in lower scores with a mean difference of 0:268 (p = 0:0053, df = 266, t = 3:3638).Severity scores are shown in Figure 3.7 and AV had the lowest score while Social Privacy had the largest score although most groups were similar. AV was the only behaviour that showed a significant difference with the other behaviours as shown in Table 3.6 with the largest difference being with Social Privacy with a mean difference of 0.2790262 (p = 7:2e 09, t = 6:3052, df = 266). This finding indicates that participants view becoming infected with a virus to have a lower level of severity than unauthorized access to their mobile device, a virus infection due to usage of peer to peer le sharing, or the loss of sensitive information through a social network. However, all of the scores were towards the upper level of the range of scores indicating that these behaviours represent somewhat sever consequences.

Controllability scores varied across behaviours with antivirus and social privacy having lower scores than locking and peer to peer as shown in Figure 3.8. Pair wise comparisons using paired t-tests show significant differences between AV and both Locking (p = 4:4e 05, df = 266, t = 4:5733) and P2P (p = 3:9e 05, df = 266, t =4:5987) as shown in Table 3.7. However, there was no evidence of difference between AV and Social Privacy or Locking and P2P. This finding suggests that participants view getting a virus in general less controllable than getting a virus through peer to
Peer le sharing. In addition protecting information shared with social networks is less controllable than using a screen lock. For the Possibility scores shown in Figure 3.9, Social Privacy had the highest average score and P2P had the lowest average score. Each of the groups were significantly different from one another with the exception of Locking and P2P and AV and Social Privacy as shown in Table 3.8. The largest average pair wise difference was between P2P and Social privacy with the mean difference equal to 0:27 (p = 1:6e 05, df = 266, t = 4:7931).

Awareness scores are shown in Figure 3.10 and varied across behaviours with Locking representing the behaviour with the highest awareness and Social Privacy representing the threat with the lowest awareness. Using paired t-tests, differences between the awareness scores were analyzed and the significance is presented in Table 3.9. Locking and Social Privacy represented the largest differences with a mean difference of: 39 (p = 7:8e 05, t = 2:4176, df = 266). These findings are in line with findings in initial behaviours we measure in mobile antivirus and locking.

6.2 **AVOIDANCE FACTORS**

Perceived susceptibility had a large range of scores across behaviours with AV rep-resenting the lower end of the spectrum and Social Privacy representing the higher end of the spectrum as shown in Figure 3.11. Through the use of paired t-tests, all of the behaviours showed significant differences between each other with the exception of AV and Locking as shown in Table 3.10. The largest mean difference was between AV and Social Privacy with a mean difference of 0:738 (p = 2:7e 08, t = 6:0634, df = 266). Hence, participants view AV and Locking as threats that the participants are less susceptible to as compared to P2P and Social Privacy. This intuitively makes sense as with P2P one is knowingly participating in dangerous behaviour and with social networks it is increasingly obvious that information leakage is happening on a regular basis.

6.3 Technology Familiarity and Risk Perception

In multiple cases, more familiarity with technology results in significant changes in perceptions. More familiarity is related with more knowledge and severity. Lower mobile usage is related with an elevated level of controllability. Figure 3.19 outlines the distribution of technology usage among all survey participants. General linear regression analyses were conducted in which the usage scores (Desktop, Laptop, Mobile, Internet, and Social Network) were used to predict each of the risk perception factors individually.

VII.SUMMARY

Overall, the results of the survey study showed that perceptions about threats and safeguards play a significant role in the usage of given security safeguards and vary across different threat scenarios. These findings support the idea that when exploring security behaviours and awareness messages, it is important to consider individual perceptions and characteristics as they can vary significantly across individuals. Additionally, people may have significantly different perceptions regarding the same risk factor across different security behaviours. For example, mobile antivirus software was found to have significantly higher perceptions of cost than screen locking.

Perception factors were obtained from both the psychometric paradigm of risk perception and the Technology Threat Avoidance Theory. Both of these models were tatted to four different security threat and safeguard scenarios. By using the factors to compare the different scenarios, it was possible to show how perceptions ranged across behaviours.

Also, factors were shown to be significant predictors of usage behaviours. Hence, it is important to explore the effectiveness of security awareness message themes across different types of behaviour as well as to consider an individual's perceptions regarding a targeted behaviour.

TABLE 1.1

Factor	Definition
Perceived susceptibility	How likely is an individual to be affected by a threat?
Perceived Severity	How severe is the threat?
Selfecacy	How well is the individual prepared to Implement the safeguard?
Perceived Safeguard effectiveness	How effective is the safeguard at protecting against the threat?
Perceived Safeguard Cost	How costly is it to perform the safeguard?

TECHNOLOGY THREAT AVOIDANCE THEORY FACTORS [3]

	AV	Locking	P2P
Locking	1.0000	-	-
P2P	0.0011	0.0043	-
Social Privacy	2.7e-08	2.8e-09	0.0312

1.2 TABLE
PERCEIVED SUSCEPTIBILITYPAIRWISE COMPARISONS USIN GPAIRED T-TESTS

CONCLUSION

The overall changes observed by intervention group as observed at the end of the study. Each of the message themes generated between 33% and 53% change in behaviour among the respective groups. The incentive group had the largest percentage of change with just over 50% change observed. The performance of the guaranteed led-payment incentive message appears to have worked better than the lottery bade incentive message in Chapter 4, which only saw 19% change in behaviour. In comparing each of the intervention message types with the control group using a Fisher's exact test resulted in evidence to support significant differences between all interventions and control group except for the regret group (Fisher's Exact, $p <$:05). However, comparing each of the intervention group's performance against each other using a Fisher's exact test failed to find any significant differences in performance.

Another way to explore the data is by analyzing changes over time. The largest increase in antivirus usage occurs the week the e-mail message is sent out. The post cards registered a small increase as did the text messages. However, it is di cult to distinguish the effects of repeated messaging and delays in changing behaviour with the effects of the mode of communication

REFERENCE

[1] M.J. deVries, M. deVries, N. Cross, and D.P. Grant. Design methodology and relationships with science, volume 71. Springer, 1993.

[2] R.G. Johnston. Tamper indicating seals. American Scientist, 94(6):515, 2006.

[3] A. Allan and P. Warden. Got an iphone or 3g ipad? apple is recording your moves, April 20, 2011. http://radar.oreilly.com/2011/04/apple-location-tracking.html, Accessed Feb. 2014 .

[4] N. Cohen. Its tracking your every move and you may not even know, March 26, 2011. http://www.nytimes.com/2011/03/26/business/media/26privacy.html, Accessed Feb. 2014.

[5] W. Enck, P. Gilbert, B-G. Chun, L.P. Cox, J. Jung, P. McDaniel, and A. Sheth. Taint droid: An information now tracking system for real time privacy monitoring on smart phones. In OSDI, volume 10, pages 1{6, 2010.

[6] N. Ungerleider. Your Smartphone could be telling advertisers how you shop and spend, August 15, 2012. http://www.fastcompany.com/3000439/your smart phone-could-be-telling-advertisers-how-you-shop-and-spend, Accessed Feb. 2014.

[7] P. Dunphy, A. P. Heiner, and N. Asokan. A closer look at recognition-based graphical passwords on mobile devices. Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10, page 1, 2010. http://portal.acm.org/citation.cfm?doid=1837110.1837114.

[8] S. Cobb. Sizing Up the BYOD Security Challenge. 2012.

[9] P. J. Connolly. iPad, iPhone Challenge Management Orthodoxy, 2012. http://www.eweek.com/c/a/Mobile-and-Wireless/Management-Orthodoxy-Challenged-by-iPad-iPhone-257619/, Accessed Feb.2012.

[10] IGillottResearch. Securing Mobile Devices on Converged Networks. http://www.trustedcomputinggroup.org/ les/resource les/DF8CF3B9-1A4B-B294-D0AE2E4ED2FFDEAD/Final iGR mobile security white paper sept 2006.pdf, 2006.

[11] M. Panzarino. Google announces 900 million android activations, 48 billion apps downloaded, 15/05/2013.http://thenextweb.com/google/2013/05/15/google-announces-900-million-activations-of-android-in-total-to-date/, Accessed Feb.2014.

[12] Apple Inc. Apples app store marks historic 50 billionth download.16/05/2013.http://www.apple.com/pr/library/2013/05/16Apples-App-Store-Marks-Historic-50-Billionth-Download.html, Accessed Feb.2014.

[13] J. Forristal. Android: One root to own them all. http://bluebox.com/wp-content/uploads/2013/08/Forristal Blackhat-US2013 nal.pdf, Accessed Feb. 2014.

[14] T. Wang, K. Lu, L. Lu, S. Chung, and W. Lee. Jekyll on ios: when benign apps become evil. In Presented as part of the 22nd USENIX Security Symposium, pages 559{572. USENIX, 2013.

[15] BuisnessWire. Riskiq reports malicious mobile apps in google play have spiked nearly 400 percent, 19/02/2014. http://www.businesswire.com/news/home/20140219005470/en/RiskIQ-Reports-Malicious-Mobile-Apps-Google-Play, Accessed Feb.2014.