ijecs
open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 09 September 2016 Page No.18216-18220

Mobile Security Awareness Efforts On User Behavior

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

1assistant Professor, Cs Department, Government Arts College, Coimbatore, Tamilnadu, India
2m.Phil Scholar, Cs Department, Government Artscollege, Coimbatore, Tamilnadu, India

ABSTRACT: *Security has long been a technical problem with technical solutions. Over time, it has become apparent that human behavior 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 behaviors 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 behavior. 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 behavior as well as response behavior 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, BYOD,IRB,Security System.*

1.INTRODUCTION

Security is a growing concern associated with the exponential growth in technology used to connect people and systems across the globe. Many technical security solutions are developed to address vulnerabilities in computer systems; however such solutions often fall short in preventing all attacks on a system. Many times, the weakness is due to the fact that humans must interact with these systems. Users of a system may not fully comprehend the complexities and vulnerabilities associated with a system resulting in human error that endangers the security of the entire system. Awareness campaigns are often times employed to raise awareness among users in order to fortify the weak human link. While awareness campaigns are readily being adopted, little is known about the effectiveness of these security awareness campaigns. This dissertation sets out to explore how effective existing techniques are at changing user behavior and also what factors may play a role in user decisions related to awareness messages.

1.1 The Need for Security

Over the past two decades, society has had a growing dependence on technology which has transformed the globe. People are undergoing a degree of change not seen since the industrial revolution. Everyone is interconnected in real-time and has access to numerous channels of information. Additionally, people produce and share information in many new ways. Hospitals are moving towards using electronic health records. Utilities are connecting plants to the grid. The advent of internet connected appliances is bringing ever expanding types of data and services onto the internet for people to access. Increasingly companies are moving to e-commerce to supplement or replace brick and mortar stores. As the speed at which technology changes increases, so to does the amount of sensitive information stored within the systems. Less than six years ago, Google Street View [8] was released, which allowed anyone with an internet connection to virtually visit the majority of streets within the U.S. Two decades ago, individuals did not need to worry about the ability of a stranger to view their house from the internet. Street View is an example of technology growing faster than policies can keep up. Along side the increase in use of technology is an increase in attacks. Companies online and offline are losing credit card information [9]. For example, in 2013 Target lost 40 million records of customer information including phone numbers, credit card numbers, and other sensitive information. Additionally, websites saw an increase in denial of service attacks, with the first two months of 2014 witnessing the largest denial of service attack ever [10] in which attackers were able to direct 200-400Gbps of attack track towards victims. The need for securing digital systems is greater now than ever before. Not only are people using more traditional computing devices (e.g. Desktops or laptops) to interact with the digital world, but have moved carrying mobile devices everywhere with them. In 2013, over a half a billion new mobile devices were added to the globe [11]. The number of mobile connected devices will exceed the world's population by 2014 [11]. The switch to using mobile devices is resulting in an increase in the amount of sensitive data contained on the devices and an enlarged attack surface. Mobile devices collect and share information about how users interact with both the digital world (e.g. browsing history) as well as the physical world (e.g. Gps location, Camera, Microphone). Additionally, the plethora of information available on mobile devices is collected and shared with service providers, application developers, and third-party advertising companies. From an organizational perspective, the increased risk is two-fold. First, with many users personally owning a variety of capable mobile devices, considerable pres-sure emerges from employees to have their organizations embrace BYOD (Bring Your Own Device) policies. Second, the perceived potential for productivity gains o ered by capable mobile devices is appealing to the organization but tempered by the risks of exposing sensitive data. According to [12], 73% of companies now have a mix of company and employee owned mobile devices. However, only 48% had implemented security measures to protect mobile devices and 21% had no plans to implement such measures in the future. Although special case studies involving BYOD have demonstrated cost savings approaching nearly half of monthly service costs [13], an article in Technology Review cast significant doubts on the overall savings of BYOD [14]. According to the article, companies such as IBM are seeing potential savings in service costs by BYOD entirely eroded if not surpassed by related support costs. Central to those support costs is the issue of risk mitigation, namely, how can an organization ensure that various mobile apps or actions by the mobile employee are not exposing sensitive information? With a company-owned device, such policies can be strictly enforced [15]. Unfortunately, the diverse array of smart mobile devices and the resulting interplay arising from employee roles and privileges makes enforcement on BYOD decidedly non-trivial [16, 17].

1.2 Raising Awareness

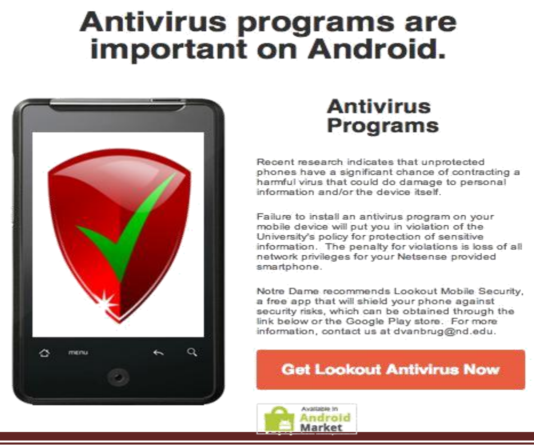
Many people have identified the need for raising awareness of security threats among workforce populations. In fact, the SANS Institute has put together the Securing The Human" set of resources [18] which claims to provide resources to develop an engaging, high-impact security awareness program". Such programs are designed to help companies build a culture of security within their organizations. Such methods include using computer based training programs, posters, e-mails, etc in order to help users identify a threat and know how to respond appropriately. However, such awareness campaigns are difficult to evaluate. Many organizations may ask if people saw certain messages posted in different areas of the company. This process would help identify exposure to a message, but not necessarily the effectiveness of the message itself. Additionally, organizations may compare levels of attacks both before and after deployment of awareness campaigns. This is highly dependent on many complex factors and does not over much insight into the effectiveness of security awareness methods. Finally, human behavior is complex with many theories within psychology literature describing how and why individuals behave in the ways they do. This thesis aims to draw on the findings from psychology literature to improve upon existing awareness techniques. One concern with the rapidly growing adoption rates of technology is that people may not have time to understand the new risks with the new technology that they are using. When a new device or service comes out, it is exciting to join and use it. However, all of the bugs may not be worked out of the system. Or, vulnerabilities may not be easily identifiable at first or even after extensive use. In any sufficiently large software or hardware system, design problems and bugs are constantly being discovered. Recently Apple introduced a fingerprint reader in their Smartphone devices. Within days, hackers had identified a simple attack that could circumvent the technology. Is it safe to assume that all users who buy the latest iphone will understand the risks associated with trusting this new fingerprint reader? Should they worry? Will such information ever reach them? As new technology grows, ideas of what is and is not safe behavior may be dif-cult to identify. Thus, it is important for an organization to ensure that risks are identified and effectively communicated to employees to mitigate risks the companies susceptible.

1.3 Methods

The following work sets out to conduct long term studies of individuals security related behaviors. We perform two in-depth targeted intervention studies to evaluate the effectiveness of different messaging techniques as well as communication methods. These studies are followed up by a survey study which explores how an individual's perception of different aspects of risk correlates with their behaviors. We also use insights gained from the survey to better inform our analysis of the targeted intervention studies. The studies will make use of multiple populations that we have access to. These include laptop users who have installed a software agent that records information about the programs they use, the network connections they make, the less they open, as well as the security measures they are using (e.g. firewall, antivirus, etc). In order to study user behavior related to smart phone security, we worked in the context of an ongoing study at the University of Notre Dame involving two hundred incoming freshmen [19]. The study provided Android Nexus S smart phones for every participant with a free unlimited data, texting, and mobile-to-mobile minutes plan in exchange for complete monitoring privileges[1]. When students enrolled in the study, they were provided with a list of all types of data that would be monitored on their devices. The study targeted a random selection of participants with effort made to balance different demographic groups within the population. As we are studying a population of self-selected college-age participants, it is important to compare and contrast our sample with an enterprise BYOD population. Complete monitoring is defined as the state of the device (battery, network connectivity) and all instances of communication (where, when, who, length) but not actual message content. We note that all monitoring is approved by our institutional IRB. First, both populations use mobile devices to keep track of personal and non-personal (e.g. school or work) data. A major difference between the two populations is the possible sensitivity of data access or data contents saved on the phone.

Employees may be more concerned with protecting company data while students may not feel school-related data is sensitive and hence may view security mechanisms as irrational as posited by [20]. From a secondary comparison, both populations follow a regular schedule in which they attend either classes or work. The regular schedule results in reoccurring social peer interactions as well as the use of the mobile device in public locations. Finally, an important point to remember is that collecting detailed information from BYOD devices of all employees in an enterprise setting is much more difficult than in a university-based self-selection study. While there are some limitations that arise from the differences between our population and a typical enterprise audience, the data we collect from students about how individuals respond to security behavior interventions will likely have implications for the future work environment. Additionally, when the phones were distributed, the study participants were also asked to all out a long-form demographic survey. The survey covered general demographic information as well as information related to prior education, personality, emotional state as well as cultural and political viewpoints. By using a combination of passive behavior monitoring, targeted interventions, and exploratory survey analysis we are able to provide some insights into individual behaviors and reactions to security awareness messages.

1.5 E-MAIL USED FOR ANTIVIRUS INVENTION



Antivirus programs are important on Android.

Antivirus Programs

Recent research indicates that unprotected phones have a significant chance of contracting a harmful virus that could do damage to personal information and/or the device itself.

Failure to install an antivirus program on your mobile device will put you in violation of the University's policy for protection of sensitive information. The penalty for violations is loss of all network privileges for your Netsense provided smartphone.

Notre Dame recommends Lookout Mobile Security, a free app that will shield your phone against security risks, which can be obtained through the link below or the Google Play store. For more information, contact us at dvanbrug@nd.edu.

1.6 FUTURE RESEARCH DIRECTIONS

The results of this research have been useful in exploring awareness message effectiveness and there are some interesting future directions the research could follow. This section outlines three areas that I believe deserve further exploration.

Social awareness study: Given the interesting relationship found between social peers and changes in behavior, it would be interesting to conduct further explorations of behavioral change in response to changes in peer behavior. One approach would be to analyze participants social interactions via social networks and look for a sample of core" individuals who have a large number of other participants as friends via social network. Then, we could provide those core" individuals with a message to distribute via their social networks regarding some new security safeguard that should be used or performed. One variable of interest could be the source of the message.

1.7 SUMMARY

Due to the growing level of dependence on technology coupled with the increasing attack surfaces available to malicious users, the need to concentrate on security is significant. While technical solutions have been developed continually as new vulnerabilities are found, there is a tendency for solutions to ignore the human factor.

This dissertation will build on research from psychology , business, and computer science to explore the effectiveness of existing techniques at raising security awareness. Additionally, empirical data has been collected and will be analyzed to explore multiple factors that relate to the effectiveness of awareness messaging schemes.

1.8 BIBLIOGRAPHY

DOI: 10.18535/ijecs/v5i9.71

1. I. Ajzen. The theory of planned behavior. Organizational behavior and human decision processes, 50(2):179{211, 1991.
2. R.W. Rogers. A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1):93{114, 1975.
3. H. Liang and Y. Xue. Avoidance of information technology threats: A theoretical perspective. MIS quarterly, 33(1), 2009.
4. Unknown. Loose lips might sink ships, Unknown. http://en.wikipedia.org/wiki/File:Loose lips might sink ships.jpg, Accessed Feb. 2014.
5. Mindful Security. Think before you link, 2014. http://mindfulsecurity.com/posters/highway/PhishingPoster.jpg, Accessed Feb. 2014.
6. E. Mauro. Lock your devices. http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurityinitiative/communityengagement/information-security-awareness,Accessed Feb.2014.
7. I. Ajzen. The theory of planned behavior. Organizational behavior and human decision processes, 50(2):179{211, 1991.
8. R.W. Rogers. A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1):93{114, 1975.
9. H. Liang and Y. Xue. Avoidance of information technology threats: A theoretical perspective. MIS quarterly, 33(1), 2009.
10. Unknown. Loose lips might sink ships, Unknown. http://en.wikipedia.org/wiki/File:Loose lips might sink ships.jpg, Accessed Feb. 2014.
11. Mindful Security. Think before you link,2014.http://mindfulsecurity.com/posters/highway/PhishingPoster.jpg, Accessed Feb. 2014.
12. E. Mauro. Lock your devices. http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity initiative/community engagement/information-security-awareness-, Accessed Feb 2014.
13. Webroot. SURVEY: Mobile Threats are Real and Costly, 2012.http://www.webroot.com/shared/pdf/byod-mobile-security-study.pdf, Accessed March 2013.
14. Enterproid. Implementing Your BYOD Mobility Strategy. 2012.
15. Apperian. Solving AndroiMultiple Personality Disorder: No Drugs Required. 2011.
16. Fraunhofer. BizzTrust, 2012. http://www.bizztrust.de/, Accessed May 2012.
17. Securing the human, 2014. http://www.securingthehuman.org/, Accessed Feb. 2014.
18. 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.
19. 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.
20. N. Ungerleider. Your smartphone could be telling advertisers how you shop and spend, August 15, 2012. http://www.fastcompany.com/3000439/your-smartphone-could-be-telling-advertisers-how-you-shop-and-spend, Accessed Feb. 2014.