International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), September 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

USER PERCEPTION OF SECURITY ON DESKTOPS/LAPTOPS AND MOBILE DEVICES (SMARTPHONES)

Khalifa Hamza[1], Kamal B. Gadanya[2], Tijjani R.Spikin[4] and Anas H.Abba[3]

[1-4]P.G Student Sharda University G.Noida, (India)
[1-4]Dept. of Computer Science and Engineering

ABSTRACT

The use of personal computer and smartphones enables users to perform great number of task, bringing improved flexibility. However, it is important to understand how users behave towards the security of their desktops/laptops and smartphones, looking into how they perceive the security of their devices. An evaluation of different task was conducted to see how users behave in security situations such as what are the activities users perform? What payment method do they use? What security mechanisms do they enforce? Which services do they grant location access? How do they select applications? Etc. To understand the user behaviors and perception in desktops/laptops and mobile devices (smartphones), a study of 100 participants were conducted on students. The results show that users prefer logging into their bank accounts with their desktops/laptops than their mobile device (smartphones), users doesn't purchase items on their smartphones compared to their desktops/laptops, users doesn't share their passwords most often compared to desktops/laptops users as well as smartphone users doesn't share their location compared to desktops/laptops users. Overall the findings show that more users are security conscious on their smartphones compared to desktops/laptops. Based on the entire findings from the research, some recommendations were presented that will help users to confidently use their devices.

I INTRODUCTION

As the field of pervasive computing and smartphones matures, it has dramatically changed the computing landscape. The use of personal computers and mobile devices is ubiquitous. A broad range of everyday activities such as shopping, socializing, reading, checking emails and video calling can be done using both personal computers and mobile devices (smartphones). However, mobile devices complement and in so many cases replace traditional computing devices such as desktops and laptops (Sterling, 2012). Smartphone applications are increasingly becoming more and more popular. Smartphone application is a term used to describe Internet applications that run on smartphones and other mobile devices. Smartphone applications help users by connecting them to Internet services that are more commonly accessed on personal computers or laptops. There has been a tremendous growth in the number and diversity of smartphone applications at marketplaces such as Google play, Android Market, Apple App store, Amazon App and BlackBerry World etc.

The advances of technology for both personal computers and mobile devices have helped make businesses more efficient and convenient. However, despite their importance, users are particularly vulnerable to constant security threats. Both computers and mobile devices are exposed to numerous kinds of threats such as malware (including worms, Trojan horses and viruses), attacks through communication mediums and data theft. Security related issues on mobile devices are different from those that are related to computers for example; a virus can infect mobile devices through an instant message (Kim &Leem, 2005). It has been stated in many studies that information security is not just a security problem, and thus these studies are being focused on human factors that affect security (Hassel &Wiedenbeck, 2004). Despite the widespread of personal computers and smartphones, there are factors that affect security behaviors of users as well as how users perceive security differently on both platforms. A study by (Leach, 2003) found out that majority of security failures is not the result of poor security solutions but poor user security behavior. There are different factors that affect security behavior among users, these factors are the things users are being told, what they see being done or practiced by other users around them and the past experience decisions that they have made (Leach, 2003). According to a study by West (2008) there are clear opinions of human behaviors that govern the way people think about security. West (2008) claims that people subconsciously think that they are less likely to be affected by computer vulnerabilities than others, and in turn leads to underestimation of security risk. He further says that people increase risky behaviors as they have different elements of security that are used such as firewalls and anti virus on their computers. West (2008) also states that, due to the limited capacity for information processing, people might not be able to think about the risks, values and alternatives. Salisbury (2003) defined security perception as "...the extent to which one believes that the Web is secure for transmitting sensitive information..." (E.g. credit card details), where the meaning of security is subjective and which can therefore vary from one person to the next. Different technology to protect computers and smartphones are available such as passwords, firewalls, antivirus, biometric authentication and encryption. Such solutions are necessary but not enough for proper protection. This is because computer security depends on the effective behavior of users (Ng et al. 2009). A survey by Ponemon (2011) shows that users worry more about security of their desktops and laptop computers than the security of their smartphones. They further stated that because of the perception about security they have on their smartphones, they don't really check the authenticity of an application before downloading it.. Also a study by chin et al (2012) found that users of smartphones are apprehensive when running privacy and financial sensitive activities on their devices. They stated that the reason behind it was as a result of fear of theft and data loss, misconception about security of their network communications and mistrust of smartphone applications. However, there seems to be little literature of comparing desktops/laptops and mobile devices (smartphones) security perception of users.Consequently there is demand for research into the role of human factors in computer and mobile information security, especially given the priority of security related issues that are been given in recent times. This research will compare and contrast computer and mobile devices (smartphones) behaviors and perceptions of users on security related issues. The outcome of the study will help users to understand security risk and recommendations on how to mitigate the risks associated in both environments.

II METHODOLOGY

To assist in exploring the research question and objectives, it is important to provide a full account of the methodology for collecting the required information. This work will present the description of the experimental study The research will be based on primary research within the boundaries of this dissertation. The methods used to achieve the primary research will have to produce necessary information in other to address the research questions.

Data collection method:

During the experimental part of this dissertation, questionnaire has been utilised to obtain the required data. From these, the data collection method chosen to evaluate the users perception of security in desktops and mobile devices was the questionnaire, mainly due to its advantage of collecting a fairly huge amount of information in acost-effective way (Saunders et al, 2003). However in other words questionnaires have its own disadvantages, which are relevant to this study. Hoyle et al (2002) identified that the response rates of questionnaires are often low, thus large amounts of questionnaires have to be managed in other to obtain an adequate response and provide reliable results. Additionally, questionnaires are very structured and their quantitative nature means that more personal answers are ignored.

Data analysis tools:

Within the survey of this dissertation, as mentioned earlier questionnaires is going to be used. This is considered as both quantitative and qualitative data's collection. SPSS was utilized for processing the quantitative data (questionnaire) in other to determine the response distributions of the survey questions and to produce the graphical illustrations of the results. This is software used for data analysis (Bryman and Burgess, 1994). The SPSS software is capable of running numerous tests that includes descriptive presentation by just selecting the appropriate command. SPSS software was used to test the validity and reliability of the data (i.e. measuring of the internal consistency of the entire data)

Data collection techniques:

Questionnaire Design

The questionnaire design is an essential part of survey research. The data that can be gained from the questionnaire can differ widely from demographic and background data to behavioral and attitudinal data. Questionnaire can therefore be defined as a list of structured questions that are designed to find out the opinions of a group of people, organisations or industries (Blaxter, Hughes and Tight, 2006). Also questionnaires comprises of questions that specific respondents complete by themselves (Fink, 2003).

Data collections:

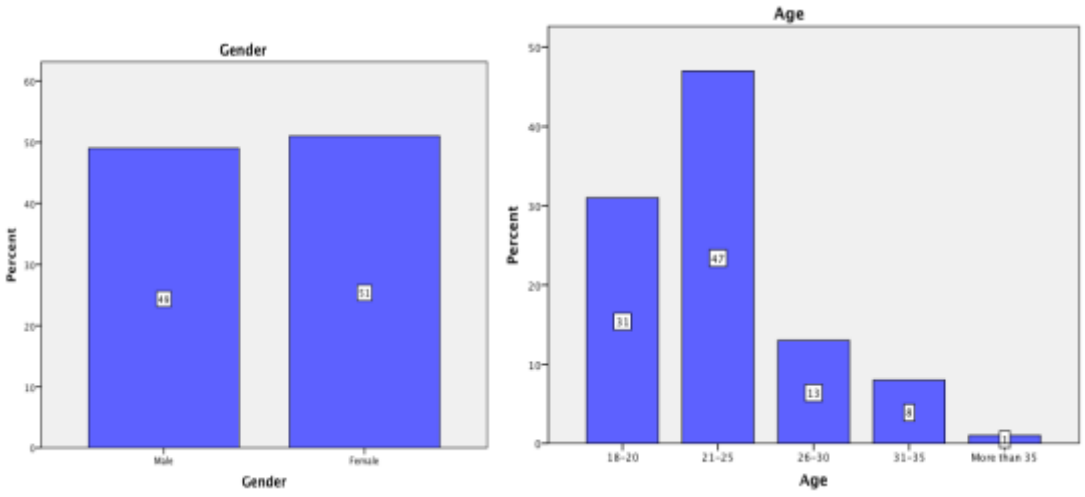
There are a number of different methods, which can be used to administer the questionnaire, this include by mail, Internet, and hand delivery or personal delivery questionnaires. However, this study will utilise personal delivery questionnaires. The advantage of personal delivery questionnaires over e-mail is that warnings against

receiving help outside can be made both verbally and also in writing (Stover and Stone, 2003). Further to that, the person picking up the questionnaire may check with the respondent to make sure he has answered all the questions himself. The authors contend that this method is not always more desirable than email questionnaires or low cost interviews but it may prove to be useful to survey researches wishing to conduct low cost surveys in a geographically compact areas.

III RESULT ANALYSIS AND DISCUSSION

Demographic analysis:

Among the 100 participants mentioned in figure the bellows, 51% were females and 49% were males, while most of the respondents were aged 18–35 (100%). All of the study participants were student from various departments and different level of study. Majority of the students were undergraduates (68%). The presented facts show that the study participants range from different level of study. Following from the sample 28% were students studying business, 23% studying management, 21% studying computing and engineering, 11% studying medicine, 7% studying Dental, 4% studying Radiology, 4% studying physiotherapy and 2% studying Law .Regarding desktops/laptops and smartphones usage, almost all of the participants were using their devices every day. Users of desktops/laptops constitutes to 77% of everyday use while smartphones constitutes to 80% of everyday use



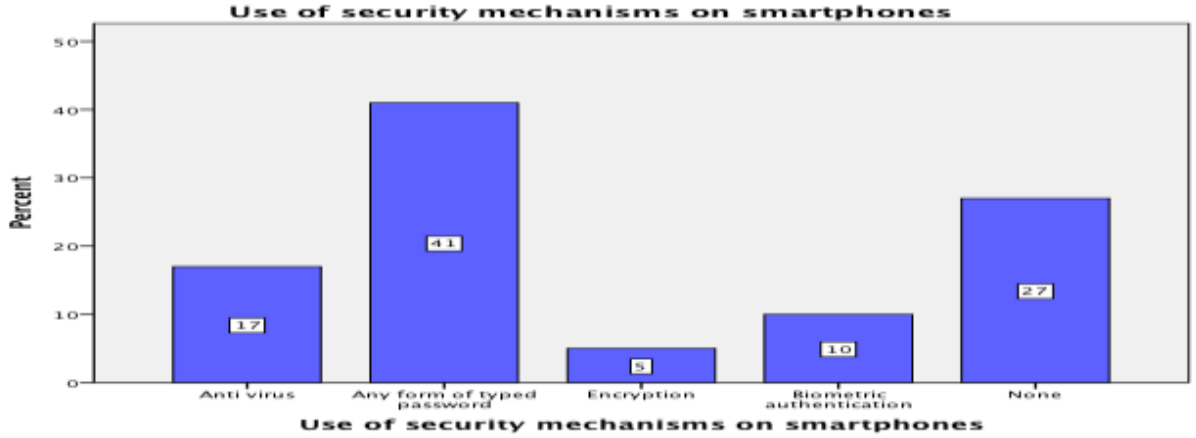
Payment method:

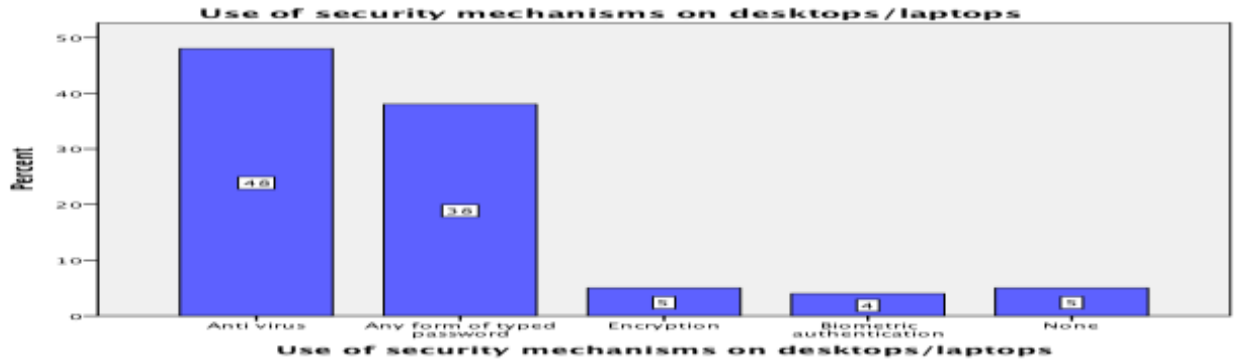
Majority of the smartphone users doesn't use their smartphones device to pay or purchase items online. It turned out that 41% of smartphone users doesn't use any payment method compared to 4% of desktop users, which shows there is a considerable difference. Additionally 26% uses PayPal on their desktops/laptops compared to 17% of mobile device (smartphone) users and 33% of desktops/laptops users uses debit card whereas 31% for mobile device (smartphone) users and so on.

International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), September 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Use of security mechanisms:

The use of security mechanisms users enforce was also considered to be an important aspect in the survey. The participants were asked about the type of security mechanism they utilize in desktops/laptops and smartphones. It turned out that 48% of desktops users uses antivirus compared to 17% of smartphones users. The result shows there is a considerable difference for the use of antivirus on desktops/laptops and smartphones. Additionally 41% of smartphone users use passwords compared to 38% of desktops/laptops users. According to IND (2012) they reported that antivirus software is not very effective for smartphones. They gave an example of an anti virus software called the Virus barriers which could be bought in the Apple's App store.





Sharing passwords:

The survey also explored whom users share their passwords with. The respondent were asked different people with whom they share their passwords with. As it can be seen from the figure below, the results were different for smartphone users and desktops users. The Smartphone user, which constitutes to 58% doesn't share their passwords with anyone, while 41% of desktops users responded similarly. The number of desktops users that share their passwords with their family was 28% whereas 23% for the smartphones users responded in the same manner. Also 16% of desktops/laptops users share their passwords with their flat mates where as 10% of smartphone users does that in a similar manner.

Installing software's;

The survey also asked participants what factors they consider before installing software's on their devices. The figure below shows that 57% of desktops/laptops users rely on the trustworthiness of the company, compared to 29% of smartphones user.

IV CONCLUSION AND RECOMMENDATION

This study investigates the perception of users on security of desktops/laptops and mobile devices (Smartphones). The most interesting findings from the results would appear to be that, when compared to perceptions about security on desktops/laptops and mobile devices (Smartphones), perceptions about security of smartphones are higher than that of desktops/laptops. There is a significant difference in the perception of security of mobile phones (Smartphones) compared to desktops/laptops. Accordingly, there is need to understand how the security and privacy has an effect of users based on their behaviors and perception at every angle before providing some recommendations on how to address and improve the security of this devices. The study was conducted with a broad number of 100 participants of both desktops/laptops and smartphones users. The data analysis shows several findings. Firstly, we find that users are not willing to perform sensitive tasks on their smartphones compared to their desktops/laptops, users are not will to share information such as location on their smartphones, users are very concerned with both security and privacy of their smartphones such as photos, videos and text messages. We also find that users doesn't share their passwords compared to desktops/laptops users as well doesn't have their online payment information on websites. The findings also reveal that users don't use security mechanisms such as antivirus on their smartphones compared to desktops/laptops. It is clear in our results that users rely on desktops/laptops to perform different activities that include sensitive information given out online, such as activities that involves money. We conclude that web page designers especially ones that deals with giving credit cards out, must take into account and show convincing informational messages about the measures taken to protect against scam and any other fraud any time the user is at a place where they are being asked to provide sensitive information. However some recommendations are proposed in other to tackle the security problems related to both environments. These findings provides and enhanced understanding of users behaviors in both desktops/laptops and smartphones environment where security behavior is important.

Critical Evaluation

Desktops/laptops and mobile devices (Smartphones) have helped make businesses more efficient and convenient due to the capabilities they provide. However, pointing out the main issue, which is the perception of users on security of desktops/laptops and mobile devices (Smartphones). The study has shown that users are more likely to perform sensitive activities on their desktops/laptops than on their smartphones. The introductory section comprised of the application of previous literatures and research data, which has been used to analyse other author's contributions on the subject. Secondly, findings of the research study which has filled a gap hence contributing to the topic, user perception of security on desktops/laptops and mobile devices (Smartphones). This rationale of creating a fit between previous researches and current findings is that it gives the reader clear understanding on the importance and scope of the research in a wider context. The research has been based on primary data technique, which was administered using questionnaires to respondents. However, the

questionnaires have been pre tested and analysed by the supervisor. This has been able to correct certain errors therefore producing accurate and concise results. The sample that was drawn for this research was from a random population selected from the Sharda University and Galgotias University. This have also aided in providing more reliable results, as there was no connection with the respondent and interviewer. Therefore, the issue of confidentiality has been addressed. Furthermore, the respondents are liable to produce honest answers, as they cannot be traced. The questions that were been investigated include, usage of desktops/laptops and mobile devices (Smartphones), activities performed, payment method, use of security mechanisms, sharing passwords, sharing location, use of online banking, installing software's, and decisions users make.

However, there are some contradictions found on previous research, which is considered to be natural to all researchers,

- T rend micro (2009) reported that many mobile users doesn't enable security software that comes with their phones and they have a notion that surfing the Internet with their mobile phones is more risk free than on their computers. On the other hand, chin et al. (2012) found that users are less willing to make purchases online or check their bank details on their mobile phones because they think computers are safer. However in our results, it shows that users are more willing to access their bank account or pay for items on their desktops/laptops rather than on their mobile devices (Smartphones)
- A nother study by Linck et al. (2006) confirmed that users pay attention to the security mechanisms on a website and thus this have effect on users perception of security but contrary to a study by Schechter et al. (2007) argued that users will still enter their credentials even when HTTPS indicators are absent. Our results shows that few users really pay attention on the security mechanisms in a website on desktops/laptops and smartphones. 14% of desktops/laptops users pay attention to the security mechanisms compared to 4% of mobile device (Smartphones) users.

In summary, this study has been able to address its set of objectives, providing credible recommendations and suggested areas of further research.

REFERENCES

1. Brian, M., (2012) Google Maps becomes the App Store's most popular free app, just 7 hours after launch [Online] Available at <http://thenextweb.com/google/2012/12/13/google-maps-becomes-the-app-stores-most-popular-free-app-just-7-hours-after-launch/>
2. Ba, S., &Pavlou, P., (2002) Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior, *MIS Quarterly*, 26, (3), pp. 243– 268
3. Bauer, H. et al (2005a) Driving consumer acceptance of mobile marketing: a theoretical framework and empirical study. *Journal of Electronic Commerce Research*, 6, (3), pp. 181–191

4. Bauer, H. et al (2005b). User Requirements for Location Based Services. In *Proceedings of the IADIS International Conference E-Commerce 2005*, 2, pp. 211–218

5. *B*en-Asher, N. Kirschnick, N. Sieger, H. Meyer, J. Ben-Oved, A. and S. Möller. (2011) On the need for different security methods on mobile phones.*In Proc. of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI)* ACM, New York, NY, USA

6. Botha, R. Furnell, S. & Clarke, N. (2009). From desktop to mobile: Examining the security experience. *Computers & Security*, 28, (3-4), pp. 130–137.[Online].

7. Bickford, J. et al., (2010) "Rootkits on Smart Phones: Attacks, Implications and Opportunities", HotMobile '10 Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, ACM, New York, NY, USA, 49-54

8. Becher, M. Freiling, F. Hoffmann, J. Holz, T. Uellenbeck, S. & Wolf, C., "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," *Security and Privacy (SP), 2011 IEEE Symposium on*, vol., no., pp.96,111, 22-25 May 201

9. Bose, A. Hu, X. Shin, K & Park, T. (2008) "Behavioral detection of malware on mobile handsets," in *MobiSys '08: Proceeding of the 6th international conference on Mobile systems, applications, and services*. New York, NY, USA: ACM pp. 225–238.

10. BSA, (2010). Global Cyber security Framework [Pdf] USA: Business software alliance. Available at <http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/Cybersecurity_Framework.ashx>

11. Bryman, A & Burgess, R., (1994) Analyzing qualitative data: Rutledge, London [Pdf] Available at http://www.tlu.ee/~katrinka/gigapeedia/data%20analysis.pdf

12. BSA, 2010.Global Cyber security Framework. [Pdf] USA: Business software alliance. Available at <http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/Cybersecurity_Framework.ashx>