EXTENDED ABSTRACT

WOMEN'S AWARENESS ON SHOULDER SURFING: HARASSMENTS OCCUR IN THE PUBLIC TRANSPORT OF SRI LANKA

TD Samarasinghe,[*,1] W.N.Sellahewa,[2] NK Samarasinghe,[3] and M.D.E.D.A Naranulpatha[4]

[1]Sabaragamuwa University, Sri Lanka
[2]Uva Wellassa University, Sri Lanka
[3]Cardiff Metropolitan University, United Kingdom
[4]Lovely Professional University, India
[*] researchassisttds@gmail.com

(Published 15 October 2021)

Abstract

Public transport is one of the most convenient and economical modes of transport in Sri Lanka. Therefore, a large portion of people use this service. Women get harassed regularly in public transport. Shoulder surfing attacks are at the forefront of this harassment. The objective of this study is to look at the extent of how much Sri Lankan women are aware about shoulder surfing. Primary data for the study was gathered disseminating a well-structured questionnaire consists of both open-ended and close-ended questions. Convenience random sampling technique was used to select the sample. From the respondents 54.5% stated that they were unaware of shoulder surfing and 23.8% of the women in the sample were victims of the attack. Women's awareness regarding shoulder surfing is very low and this research provides information on how to regulate the use of social media in public transportation by increasing women's awareness of social engineering attacks.

Keywords: Social engineering, shoulder surfing, women harassment

1. Introduction

Women in Sri Lanka always have been tempted to use public transportation to facilitate their daily commute. The safety of women in public transportation has long been a major issue in our society. Answering this problem is a very difficult challenge. In addition to the physical abuse of women on public transportation, the dark side of technology has recently led to new forms of harassments (Choi et al., 2016). This is a new kind of stress aggravation for women (Adebimpe et al., 2019).

Most women are accustomed to use social media such as Facebook, WhatsApp and Instagram to alleviate their anxiety and fatigue while traveling (Gelms et al., 2021). The excitement of the virtual world that social media creates make the users unknowingly isolated. Further, wearing headsets and headphones helps to completely separate them from the outside world. This reason alone is sufficient for the users to be unaware of shoulder surfing. Addictiveness into social media make a great opportunity for shoulder surfers. For a case in point, consider a woman who is addicted to her mobile device and to social media. A person is eyeing her mobile device and gains a better understanding of the woman's social media accounts without her concern (Dhanashree et al., 2015). Then that person search the woman's social media accounts, downloads all available public photos

and creates a fake account. Upload the photos to a pornographic website and ask a ransom to delete the photos. Moreover the person can hack her social media accounts by sending a phishing attack, or can steal her identity. To what extent are women aware of assaults using such technology? This is just one example of a possible shoulder surfing attack on women using public transportation (Hanif et al., 2019).

The purpose of this research is to recognize shoulder surfing awareness of women who are using public transportation. To increase the dignity of women in the society, to open eyes of the authorities about the harassment which women face in the cyber world and to educate women about social engineering attacks.

2. Literature Review

According to Kearl et al (2012)'s study, street harassers are more likely to harass women in public. It also claims that women and children are not safe in public transit at a higher rate than males because people try to take a peek at them, follow them, check their phones, and approach in an improper manner (Gelms et al., 2021). Because there are so many criminals who take bags and cellphones, critical and personal data is stolen, the person who took it can utilize it to their advantage (Yogita et al., 2017). As a sort of attack against the human element, social engineering entails getting the target to divulge information or take activities they shouldn't. Nohlberg et al (2008) has focused Understanding, quantifying, and defending social engineering. Getting a better grasp for social engineering involves learning about its definition and how it operates. This is accomplished through studying past work in the field of information security, as well as other relevant areas of research (Goucher et al., 2018). "Shoulder surfing is a type of observation attack," says the author Gao et al. (2010). Because of the capacity to work in public locations, the risk of sensitive information being seen by an intruder has grown. The combination of probability and consequences is known as risk. A threat of exploiting a vulnerability and generating an impact is required for risk, there is no danger if these do not exist (Ohya et al., 1994). The chance that a shoulder surfer may view, comprehend, and record sensitive material in a way that harms the information owner is crucial in determining whether working on that document in a public area is acceptable (Simões et al., 2019).

3. Methodology

Primary data for the current study have been gathered disseminating a well-structured questionnaire which consists of both open-ended and close-ended questions. Survey method was used and the data for the current study has been gathered using a Google form. The Google form was distributed via emails and social media sites such as Messenger, Viber and WhatsApp. The questionnaire was designed to allow respondents to respond as quickly and easily as possible arranging the answers following likert scale method. The survey was conducted during five months' time from August 2020 to December 2020. Convenience random sampling technique has been used to select the sample. 110 questionnaires were disseminated among women of all ages who use public transportation and who use mobile devices. It was able to extracted 100 responses that can be useful for the current study. Gathered data have been analyzed by following mixed method. Basic statistics were generated manually and answers received for open-ended questions have been analyzed descriptively. The final pool of the sample represented the respondents were in the category of women who use public transportation and at the same time use mobile devises to facilitate their work.

4. Results/Analysis and Discussion

The majority of the respondents (68) were from the category 21-29 years of age. Pupils under 20, the adolescents, and senior women in the 50-59 age group were under-represented. We can attribute this to the fact that despite the use of public transportation in those age groups, the use of smart devices is very low.

Findings show that people between the ages of 21-29 and 30-39 are more likely to use social media while traveling. According to the responses WhatsApp is the most used social media and subsequently, Facebook, Instagram, LinkedIn, Viber and Twitter are used. These platforms are very important to build relationships but because of the technological impact that comes with it nowadays, positive conducts such as reading books have slowly faded away as people have made it a habit to waste their time on social media.

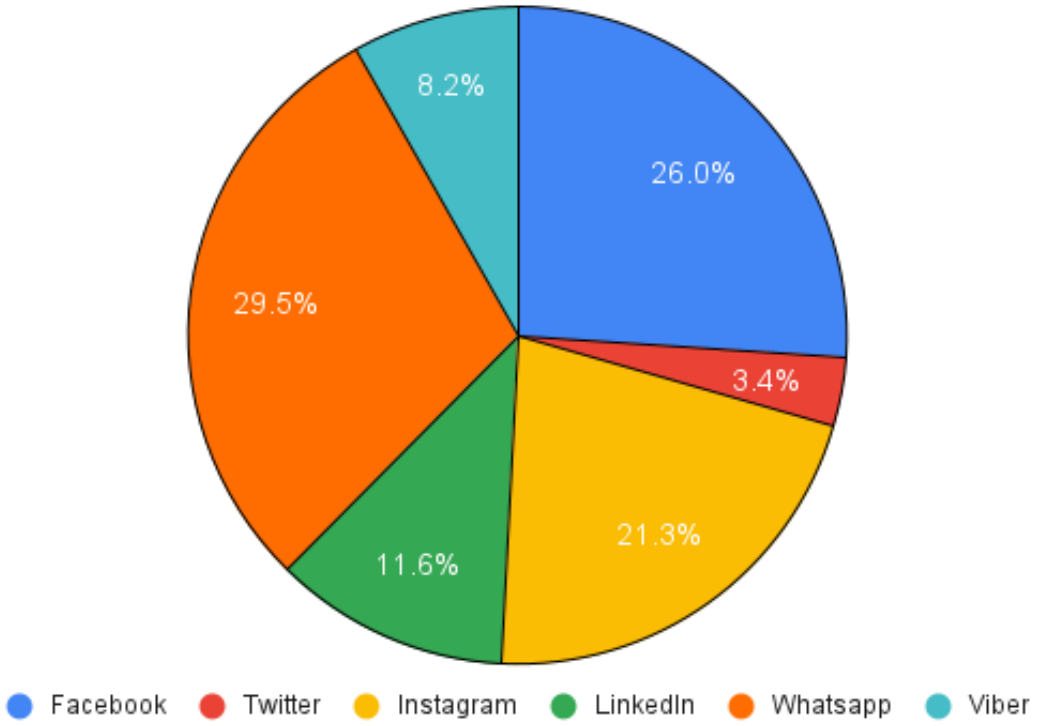

Figure 1. Most Popular Social Media among Respondents.

People use these platforms as a medicine to soothe the afflicted mind on a busy day. Therefore we can depict that many people are addicted to using it. Findings describes that many people have a high connection with social media when traveling. Because of this interaction, many people are unaware of their surroundings. Wearing headphones aid to expel the person from the world around them.

The most common modes of transport used by the respondents are bus, train and cab services respectively and most of the respondent's use these services are between 6.00 am - 8.30 am and 4.30 pm - 6.30 pm. Due to the high number of passengers traveling in buses and trains, there is almost no privacy in these services. According to the findings most shoulder surfing attacks happens in these two time periods. Only 45% of respondents are aware about shoulder surfing. And from that percentage only 10% have stated about post shoulder surfing attacks happened to them and 34.7% of the respondents know whom to inform when a shoulder surfing or any other social engineering attack happens.

With the advancement of technology, mobile devices have become more and more technologically sophisticated and user friendly at the same time. The device's display plays a major role when it comes to choose a smart device. Increased display size means more interaction with the device. Bigger displays have a greater probability not only to be visible to the owner but to the surrounding environment as well. Thus, we can say that the incidence of shoulder surfing attacks increases with bigger displays.

Single sign on (SSO) is used to access multiple social media platforms using one password and one account. The advantage of using this is that you do not need to remember a large number of passwords. The main disadvantage here is that when an unauthorized person finds out this password, they will get the access to several social media accounts. Using SSO helps the shoulder surfers to attack several social media accounts of a particular person. Most people in this group have a certain level of education. Most are graduates. Despite their level of education, they have no proper education about "shoulder surfing" social engineering attacks and how to prevent them .because of this many have become victims of shoulder surfing attacks. Password breaching, social media accounts hacking, identity theft and stealing public photos have become the most popular post shoulder surfing attacks. Even many have admitted that they post photos publicly in social media that aids these kind of cyber-attacks in many ways.

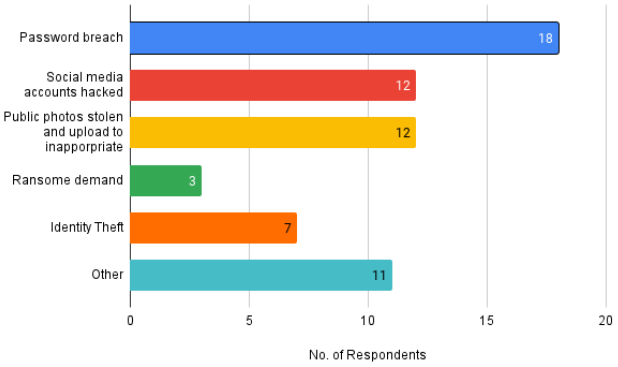

Figure 2. Post Shoulder Surfing Attacks Which Respondents faced.

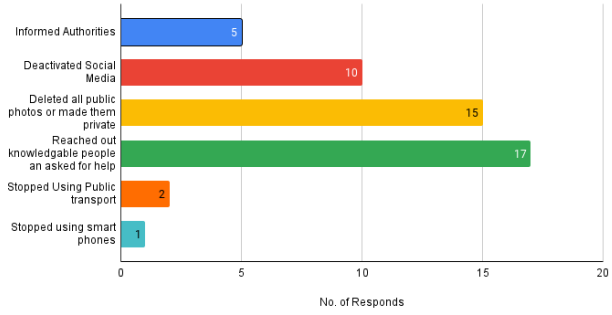

Figure 3. Actions taken by Respondents after a Shoulder Surfing Attack.

Sri Lanka CERT | CC is a national liaison centre for all cyber security matters and receives numerous incident reports / complaints related to the country's national cyberspace. Sri Lanka CERT has received information on social media related incidents, if we refer to Sri Lanka CERT's Annual Activity Report for 2020, most of the reported incidents fall into the category of social media related events and on average more than 1000 reports are reported every month. As usual, the number of social media events was the highest on Facebook. Many have stated that they don't know where to report if an incident like shoulder surfing happened. And they have taken numerous actions after an incident happened like deactivating the accounts, deleting images and stopped even using mobile devices.

The first recommendation is to make autonomy that will make sure you have no need to search personal content on public transportation. As Public we cannot stop all prying eyes and it is better not to give personal information to those who do not know, make a habit of reading or listening to music while traveling. Turn the screen of the smart device away from the person next to you, create a physical barrier between your screen and that person. Use the smart device's biometric system such as finger print scanner and face detection. These technologies provides a quick, easy, and secure way to access your accounts without revealing your password. Always be mindful of your surroundings when you use social media. Conduct workshops to educate women about shoulder surfing, how to identify attacks and respond to them. Furthermore, organize workshops on all the advanced technologies women need to know when using password protection, SSO and smart device.

5. Conclusion and Implications

Research has shown that the "today" of women has changed radically due to the rapid transformation and spread of technology. Restricting access to social media platforms will severely affect them as technology and social media are an integral part of their lives. These effects should be taken

into account when formulating strategies to prevent and intervene in the harassment of women using social media while using public transportation. This research evaluates the suggestions and recommendations of women who have been harassed on social media, analyze their experiences of harassments and then explore their recommendations and future solutions to this complex social problem. Evaluate current proposals on education, technological tools and policies and make some firm recommendations on identifying gaps or anomalies and finally nurturing social engineering awareness, directing women to use technology and public transportation services deprived of hesitant. We need to restore the good moral values that are disappearing from Sri Lankan society and create people with good attitudes. Searching for the personal belongings of others is an ignorant trait. People need to be educated at the school and social level to respect the privacy of others.

References

Dhanashree Chaudhari, (2015) A Survey on Shoulder Surfing Resistant Text Based Graphical Password Schemes. (2015), 4(11), 2418-2422.

Choi, D. (2016). Password Authentication Scheme Resistant to Smudge and Shoulder Surfing Attack in Mobile Environments. *Asia-Pacific Journal of Multimedia Services Conver*

Goucher, W. (2018). Know Your Enemy: Shoulder Surfing. ITNOW, 60(4), 32-33.

Gao, H., Ren, Z., Chang, X., Liu, X., & Aickelin, U. (2010). A New Graphical Password Scheme Resistant to Shoulder-Surfing. *SSRN Electronic Journal*.

Gelms, B. (2021). Social Media Research and the Methodological Problem of Harassment: *Fore grounding Researcher Safety. Computers and Composition* 59, 102626.

Hanif, S., Sohail, F., Tariq, A., & Imran, M. (2019). A New Shoulder Surfing and Mobile Key-Logging Resistant Graphical Password Scheme for Smart-Held Devices. *International Journal Of Advanced Computer Science And Applications* 10(9).

Kearl, H. (2012). Stop Street Harassment. Createspace Independent Pub.

K, M., Yogita, B., Dhanashree, B., & Rani, D. (2017). A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme. *IJARCCE* 6(3): 1006-1009.

Nohlberg, M. (2008). Securing information assets. Department of Computer and Systems Sciences (together with KTH), Stockholm University.

Por, L., Adebimpe, L., Idris, M., Khaw, C., & Ku, C. (2019). LocPass: A Graphical Password Method to Prevent Shoulder-Surfing. *Symmetry* 11(10): 1252.

Ohya et al., 1994 Shoulder Surfing and Keylogger Resistance using Two Step Graphical Password Scheme. (2016), 5(6), 2395-2399

Simões, R., & Silveirinha, M. (2019). Framing street harassment: legal developments and popular misogyny in social media. *Feminist Media Studies* 1-17.