Smartphone Cyber Security Awareness in Developing Countries: A Case of Thailand

Feren Calderwood(✉) and Iskra Popova

Department of Computer and System Sciences, Stockholm University,
NOD-Huset, Borgarfjordsgatan 12, 164 55 Kista, Sweden
feca4014@student.su.se, ipopo@su.se

Abstract. Cyber security awareness among smartphone users is becoming one of the main challenges of cyber security in both developed and developing countries. This paper focuses on Thailand, a developing country that is ranked among the riskiest countries in the world with regards to cybercrime. Through a survey exploring the knowledge and practices of Thai student smartphone owners, as the young population is the largest user group, we seek to estimate the level of their cyber security awareness about the most common risks. The findings reveal that they are most susceptible to identity theft or data compromise, while they were on the whole found to have a higher level of security awareness than students in other countries. We argue for Thailand's digital economy to be sustainable, ICT4D projects need to extend their focus to this population of smartphone users to increase security awareness.

Keywords: ICT4D · Cyber security awareness · Smartphone users
Developing country · Thailand · Risk

1 Introduction

With the increase of cyber-attacks and their diversification, so is the threat to the growth of the digital economy in both developed and developing countries. Cyber-attacks are specifically challenging for developing countries. At the same time that they try to build or further develop their information and communication technology (ICT) infrastructure, they also have to build resilience to ward off these threats [1]. It is critical that they do so and align with Goal 9 of the UN Sustainable Development Goals[1], to ensure that their digital infrastructure will become sustainable.

In the recent years the number of smartphones in many developing country shows a trend of constant growth. While smartphone operating systems have been increasingly designed with inbuilt security to be enabled after acquiring a smartphone device, the accountability of caring about and practicing cyber security is placed upon the individuals. For people in developing countries, many will get their first Internet access through smartphones. Besides being exposed to attacks common to computers they are threatened by other events that come from the specifics of these small devices. The

[1] Goal 9 concerns "build a resilient infrastructure, promote sustainable industrialization and foster innovation" and includes targeting upgrade of infrastructure by 2030 to make them sustainable.

R. Zitouni and M. Agueh (Eds.): AFRICATEK 2018, LNICST 260, pp. 79–86, 2019.
https://doi.org/10.1007/978-3-030-05198-3_7

human element in cyber security should be addressed through estimating the cyber security knowledge and practices of the end users, and through providing the relevant education and training. This is in particular important for developing countries with significant penetration of smartphones used for Internet access and the expansion of mobile services offered by various actors in the society.

There is plenty of research dedicated to estimating cyber security knowledge and practices of smartphone users. Most of it has been carried out in developed countries [2–5] with very few in the developing world [6]. The studies show that the smartphone security practices are weak and that their cyber security knowledge poor. However, no published articles in English dealing with cyber security awareness of smartphone users in Thailand have been found.

Thailand is a middle-income developing country in South East Asia. Its government has digital development high on its agenda and has established its Digital Economy and Society Development Plan [7] that sets out to extend Internet access and enable e-commerce as well as e-payments. It received support under the auspices of the International Telecommunication Union (ITU) through the ICT for development (ICT4D) project No. 9THA150306 to build human capacity in cyber security and critical infrastructure protection [8]. While this project focused on strengthening the capacity of the government agencies, not visible on the cyber security roadmap in Thailand is the role of end users, and specifically, smartphone end users as 82% of them use the phones for accessing the Internet [9]. Out of the whole population in Thailand accessing the Internet through smartphones, 83% are 18–34 years old, and only 27% are 35 + years old with the smartphone owner group more likely having secondary or higher education (82%) [10].

This paper presents the research about cyber security awareness of Thai students performed as a part of the thesis work at the ICT4D master programme at Stockholm University [11]. The next section provides an overview of the smartphone cyber security risks followed by the section describing the methodology and the limitations. The findings and the conclusions are presented in the last two parts of the paper.

2 Smartphones Cyber Security Risks

The European Union Agency for Network and Information Security (ENISA), acting also as regional advisory body for Asia [13] identified the top six risks for the smartphone users [14].

Data leakage Resulting from Device Loss or Theft: Data leakage can have a severe impact as 97% of smartphone users according to the Kaspersky global survey [15] store a combination of self-created photos/videos/music, personal email, SMS, passwords/PIN codes, phone contacts, banking details. Users are particularly vulnerable if they don't use any form of authentication on their device.

Unintentional Disclosure of Data: This is related to mobile applications gaining excessive permission to the phone content by which it may disclose this data online or to the developer. Using unprotected transmission of data via public Wi-Fi spots can also cause data disclosure.

Attacks on Decommissioned Phones: Digital forensic software has advanced so that data can be retrieved from phones even if they have been factory reset before being re-sold, thrown away or given to a mobile phone decommissioning centre. It is usually recommended that after the factory reset, the user uploads fake data and performs the factory reset again. If the procedure is repeated several times, the probability of discovering the original data is drastically reduced.

Phishing Attacks: An attacker collects user credentials, such as passwords or credit card numbers, using fake applications, SMS or email messages that seem genuine. Smartphone users can be susceptible if they are unaware of how to detect malicious e-mails, SMS messages or forged web links asking for passwords or other sensitive information.

Spyware Attacks: Malicious applications (malware) that can record, steal and transfer data to its creators, the attacker, can end up on the smartphone through downloading and installing applications from untrusted sources. Threats usually come from third-party app stores. However, even apps on Google Play or Apple Store can occasionally mask malware.

Network Spoofing Attacks: This commonly happens in free Wi-Fi hotspot environments, whereby an attacker gives a Wi-Fi a name that may seem legitimate to observe the data being sent and received by those who connect to it. Even legitimate open Wi-Fi networks can be used for such activities. Often when these networks are password protected, the access to the password can be easily obtained or guessed.

3 Methodology and Limitations

The research sets out to explore cyber security practices of student smartphone users in Thailand, to discover the aspects where there is a lack of knowledge and to recommend directions for development of future programmes in raising cyber security awareness. The objectives are broken down as follows.

- Identify the top cyber security risks for Thai smartphone student end users
- Estimate the level of protection that their practices provide against cyber-attacks;
- Depict the cyber security aspects requiring increased cyber security awareness.

A questionnaire gathered the information on security practices of Thai students who own smartphones. The same data collection method was already used in the majority of the research on the same topic, [4–6]. This is a productive method for data collection when the information required is relatively brief and uncontroversial and can be obtained directly from the informants [15]. Simple and short questions on how smartphones are used or what actions users take when there is a danger from cyber-attacks provide information about cyber security knowledge, attitudes and behaviours without any sensitive issues being tackled.

A web platform easily accessible with a smartphone was used to administer the questionnaire. Answers from the Thai students were collected in the autumn of 2016 through HaiSurvey, an incentive-based online system operated by the public opinion expert agency W&S Asia who provided the translation of the questions in Thai language and made them available to a panel of 10,000 potential respondents.

The ethical issues were addressed by presenting to the participants an introductory text that described the purpose of the research, the rights to voluntarily participate in the survey with the possibility to exit at any time and by emphasizing their anonymity was guaranteed. The HaiSurvey system protects the anonymity of the participants and does not capture nor share any personally identifiable information with the researcher. Because of the limited budget of the student researcher, the following limitations are present.

1. The questionnaire consists of 24 questions. 17 of them dedicated to exploring the Internet usage and the security practices, two screening questions filter respondents who are student smartphone owners, and five questions collect demographic data.
2. All the questions are closed with five of them having an open field.
3. The number of valid responses is 115.

4 Results

The questions included in the online questionnaire are based on the work previously done by [4] and [5]. Table 1 lists the questions in the questionnaire and the responses obtained with the two screening questions not included.

The analysis of the demographics data obtained with Q1 to Q5 shows that that the sample can be considered as approximately representative of the population of Thai students although the sampling strategy used was not a strictly representative one. According to [16] the majority of Thai students start with tertiary education at age 18 or take some professional education. This is in support to having the majority or 74% of our respondents at the age 19 to 25. This number is aligned with the responses about the level of education where 76% are at the undergraduate level or take the professional education. The statistics from 2015[2] shows that 58. 3% of the students in the tertiary education in Thailand are females. This is very close to the gender distribution in our sample with 60% females. The distribution of the students according to the regions is similar to that of the population in Thailand[3] not taking into account Bangkok that houses the majority of the tertiary institutions. Regarding the operating systems (OS), our distribution with 60% Android and 40% iOS is not far from the statistics[4] showing personal use of Android is 59% and of iOS 31%.

The responses to Q6 to Q10 picture Thai students having large range of devices, a variety of applications installed on the smartphone with significant amount of sensitive data stored. The majority spend on the Internet more than two hours per day.

[2] Source: http://data.uis.unesco.org/#, Percentage of students in tertiary education who are female.

[3] Source: http://www.citypopulation.de/Thailand-Cities.html, Thailand regions.

[4] Source: https://www.statista.com/statistics/563664/thailand-types-of-smartphone-operating-systems-used-for-personal-purposes/, Smartphone OSes used for personal purpose.

Table 1. The questions in the questionnaire and the responses obtained

Q#	Questions	Responses
Q1	What is your age?	19 to 25 (74%); 26 to 34 (26%)
Q2	What is your gender?	Male (39%); Female (60%); Other (1%)
Q3	What part of Thailand do you live in?	Central including Bangkok (56%); North, Northeast (30%); East, West, South (14%)
Q4	What level of education are you enrolled in?	Undergraduate (60%); Master level (24%); Other professional degree (16%)
Q5	What OS does your smartphone have?	Android (60%); iOS (40%)
Q6	Please tell us which electronic devices you own?	Smartphones (100%); Computers (78%); Microwave (73%); Dishwasher (0%)
Q7	How many hours per day on average are you connected to the Internet using your smartphone?	More than 2 h (92%); Between 1 and 2 h (6%); Less than one hour (2%)
Q8	How do you access the Internet using your smartphone? Please rate 1-5 in order of most often to never.	Mobile data plan: (47% most often, 30% often, 16% not very often, 3% rarely, 4% never); Home password protected network (40% most often, 36% often, 13% not very often, 6% rarely, 5% never)
Q9	What type of data do you store on your smartphone?	Photos (96%); Emails (86%); Passwords: social networks, email accounts (69%), bank accounts, credit card numbers (63%)
Q10	What types of applications do you use on your smartphone?	Shopping (72%); Transportation (63%); News (57%); Social (89%); Communication (77%); Games (80%); Finance and banking (79%); Entertainment (79%); Productivity (38%); Tools (48%); Security (42%)
Q11	Where from do you install your mobile applications?	Physical mobile store (6%); Authorized online shop, iTunes or Google Play (74%); Any site where the needed application can be found (20%); Other (0%)
Q12	What type of access protection do you use on your smartphone?	Password with capital and small letters (32%); Password with mixed letters and numbers (33%); Password pattern (10%); Biometrics (19%); None (6%)
Q13	Have you set up access protection to any of your smartphone applications?	Yes, to all of them (17%); Yes, to some of them (56%); No I have not (27%)
Q14	Have you got rid of an old smartphone? If so, what did you do with it?	Gave it or sold to a family member or a friend (54%); Gave it or sold it to an unknown third party (28%); Threw it in the garbage (2%); I have never got rid of my smartphone (16%)
Q15	If you answered yes to the previous question, did you do this beforehand?	Factory reset my smartphone (65%); Factory reset the smartphone, then loaded fake data on to the phone and factory reset the smartphone again (12%); Repeat the previous option several times (6%); I never got rid of it (17%)
Q16	Do you click on links in e-mails or SMS from unknown senders?	Always (49%); Sometimes (43%); Never (8%)
Q17	Do you check what permissions applications require when installing them?	Always (75%); Sometimes (22%); Never (3%)
Q18	Do you read news about smartphone security?	Always (62%); Sometimes (36%); Never (2%)
Q19	Have you ever misplaced your smartphone?	Always (20%); Sometimes (56%); Never (24%)
Q20	Have you ever decided against the using of an application because the app wanted to access your personal data?	Yes (84%); No (11%); I do not know (5%)
Q21	Do you have some security software installed on your smartphone?	Yes (74%); No (21%); I do not know (5%)
Q22	What kind of security software do you have installed on your smartphone?	Anti-virus (73%); Anti-theft (42%); Ant-spam (39%); Data encryption (34%); Firewall protection (26%); Other (0%)

Two specific findings about the cyber security awareness standout 1) students show a high likelihood of being victims of social engineering and phishing; 2) they highly appreciate their privacy and protect themselves from spyware. These results are due to Q16 and Q20. Figure 1 shows the distribution of the answers with the dark areas presenting the negative habits or bad security practices leading to high risks. The fact that the majority of the downloaded applications are from an authorized app store, as per the answers to question 11, indicates a rather low risk from spyware attacks. The answers to question 17 shows that three-quarters of the respondents always pay attention to the permissions asked by the applications, additionally show their concern about privacy.

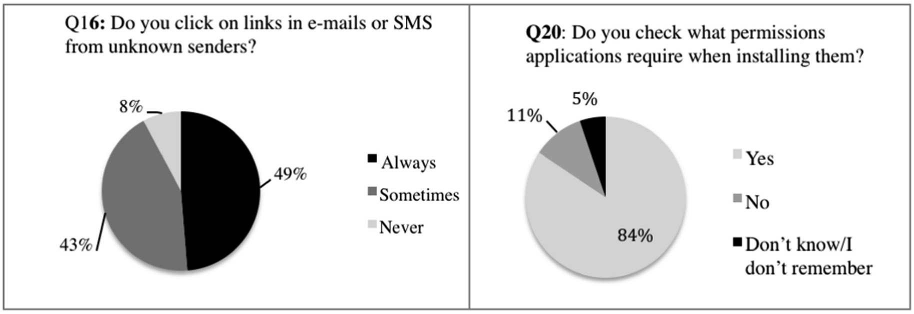

Fig. 1. Distribution of the responses to Q16 and Q20, the dark areas showing negative habits

Regarding other aspects of smartphone cyber security, the findings point to a moderate level of security awareness. According to the answers to question 8, students most often or often connect to the Internet via a protected home Wi-Fi network and rarely to public ones, thus avoiding the risk of network spoofing attacks. The risk from leakage of data due to displacement or loss of the device is not that high because a large portion of respondents use appropriate passwords for locking the screen and for accessing the applications (questions 12 and 13). Also, the responses to question 19 show that not too many respondents are prone to always displacing their phone (only 20%). The risk from attacks on a decommissioned phone is moderate as per the answers to questions 14 and 15 about the respondents getting rid of the old phones either in the most proper or in a proper manner. Questions 18, 21 and 22 asked about the interest in cyber security. The answers showed that the informants having moderate interest in following the news on cyber security, however many of them have some security software installed on their device.

5 Conclusion

According to the reported security practices and behaviours, these Thai students exhibit a moderate level of awareness about cyber security risks except for the risk from phishing attacks about which they have low awareness, and the risk from spyware, where they have high knowledge on how to protect themselves. The respondents show a higher concern and knowledge about the threats from downloading and giving permissions to applications than most students in developed countries [2–5]. When it comes to the threats from phishing attacks, their unawareness is higher than that of students in developed countries. 82% of Thai students who either always or sometimes click on links in phishing emails is much higher when compared with 58% of respondents in the UK not being familiar with phishing [2], and 49% of students in Australia not considering that phishing emails could have negative consequences [5].

Humans are always the weakest link in the cyber security chain in any country. The vulnerability of developing countries is higher due to the limited resources they have to address all the aspects of cyber security, as is the case with Thailand. Therefore we suggest that ICT4D programmes involve training and education of end users. The programmes should be based on the findings of the knowledge gaps and bad practices. They should be led as a joint initiative by the government, mobile industry and education sector. Government has the power to give the mandate for the industry and education system to play an active role in building the e-society. The mobile industry promotes their brand value through providing education in the form of smartphone risk simulations games that consumers play. This is supported by the findings by Fung et al.'s [17] pilot study which showed that e-learning, through a game, significantly increased the students more in depth knowledge and understanding of information security.

Through being capable of protecting themselves against cyber-attacks, the smartphone users contribute towards better cyber security at a national level. This in turn has a positive impact on building confidence and trust in the mobile services offered and contributes to the sustainability of the online economy.

References

1. Tagert, A.C.: Cybersecurity challenges in developing nations. Doctoral dissertation. Carnegie Mellon University (2010)
2. Lazou, A., Weir, G.: Perceived risk and sensitive data on mobile devices. In: Weir, G.R.S. (ed.) Cyber forensics, issues and perspectives, pp. 183–196. University of Strathclyde, Glasgow (2011)
3. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measure user confidence in smartphone security and privacy. In: Symposium on Usable Privacy and Security (SOUPS) (2012)
4. Mylonas, A., Kastania, A., Grizalis, D.: Delegate the smartphone user? Security awareness in smartphone platforms. Comput. Secur. **34**, 47–66 (2013)
5. Imgraben, J., Engelbrecht, A., Choo, K.R.: Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. Behav. Inf. Technol. **33** (12), 1347–1360 (2014)
6. Ophoff, J., Robinson, M.: Exploring End-User Smartphone Security Awareness within a South African Context. Information Security for South Africa (ISSA) (2014)
7. Thailand Digital Economy and Society Development Plan. http://www.digitalthailand.in.th/drive/Digital_Thailand_pocket_book_EN.pdf. July 2016
8. ITU project 9THA150306 website. http://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9THA15030. July 2016
9. Thailand Internet User Profile 2015. EDTA (2016)

10. Internet Seen as Positive Influence on Education but Negative on Morality in Emerging and Developing Nations – Internet Usage More Common among the Young, Well-Educated and English Speakers. http://www.pewglobal.org/files/2015/03/Pew-Research-Center-Technology-Report-FINAL-March-19-20151.pdf. 16 Apr 2016
11. Calderwood, F.: Cyber security risks for smartphone users in Thailand. Master thesis. Stockholm University (2017)
12. Choucri, N., Madnick, S., Ferwerda, J.: Institutions for cyber security: international cyber responses and global imperatives. Inf. Technol. Dev. **20**(2), 96–121 (2014)
13. ENISA: Critical Applications – Smartphone Security Top Ten Risks. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks. May 2016
14. Kaspersky Lab: One in every six users suffers loss or theft of mobile devices, 21 October 2013. http://www.kaspersky.com/about/news/press/2013/one-in-every-six-users-suffer-loss-or-theft-of-mobile-devices. July 2016
15. Denscombe, M.: The Good Guide Research Guide for Small-Scale Social Research Projects, 4th edn. Open University Press, Maidenhead (2010)
16. OECD/UNESCO. Education in Thailand: An OECD-UNESCO Perspective, Reviews of National Policies for Education. OECD Publishing, Paris (2016)
17. Fung, C.C., Khera, V., Depickere, A., Tantatsanawong, P., Boonbrahm, P.: Raising information security awareness in digital ecosystems with games – a pilot study in Thailand. In: 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies, pp. 375–380 (2008)