EDUCATIONAL AND TRAINING MODEL OF SECURITY AWARENESS ON MOBILE DEVICES FOR STUDENTS'

DZAIROL ADZRIEM BIN DIN

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

AUGUST 2012

Alhamdulillah… thank you to Allah. Because of Him, I manage to reach at this level. I lovingly dedicate this project to my beloved family, especially to my Dad and Mom for instilling me the importance of hard work and higher education. Not forgotten for your financial and moral support till your son got to complete this study. Thank you so much.

I also dedicate this to my respected supervisor, Dr. Norafida Ithnin who gives me knowledge, advices and encouragement towards the project.

Dear fellows' friends, thanks for your kindness and moral support. Always helping each other and motivate each other. Thank you so much. Those sweet memories we all together will never be forget.

ACKNOWLEDGEMENT

"Bismillahirrahmanirrahim"
In the name of Allah, the Most Gracious,
the Most Merciful and the Most Compassionate.

Alhamdulillah, all praise to Allah for the strengths and His blessing to completing this research and thesis writing. My special appreciation goes to my supervisor, Dr.Norafida Ithnin, who supervises in term of giving a useful knowledge and constant support. Her invaluable help in constructive comments and suggestions throughout the study have contributed to the success of my research. Not forgotten, to express my appreciation to all lecturers of computer science faculty and dearest UTM's students who contributed to this research finding and also for their co-operations.

Sincere thanks dedicate to all my lovely friends, especially *"Dunia ScS friends"* and *"Information Security Classmate"* for their moral support and kindness during my study. All the sweet memories will never forget and thanks for the friendship and brotherhood.

Last but not least, deepest gratitude goes to my beloved parents; Mr. Din B. Sabu and Mrs. Zainab Bt. Omar and also the rest of my family for their endless love, prayers, encouragement, spiritual and financial help and support. To those who indirectly contributed to this research, your kindnesses are highly appreciated. Thank you so much.

Sincerely: DzairolAdzriem , 2012

ABSTRACT

Nowadays technology has rapidly evolving. In mobile device technology, since it has become a vital part of daily human life, the developers keep upgrading devices and software to perform better. Smartphone has replaced cellular phone and it is widely use due to the advance technology offered in the device. More similarity functions and features of smartphone with computer are turning smartphones to be exposed to numerous security threats such as malicious code (including virus, worm and Trojan) and other vulnerabilities. Students often obsess in having an advance technology device but unfortunately they lack of security awareness on their devices. Lack of security education and feeling the device is secure enough has lead them to ignore to apply security features to the device. Due to this matter, a study was conducted towards UTMs' student by distributing pre-survey question to identify their current state of awareness, concern and knowledge of the technology. The result found that they still at low level of awareness concern and necessarily to undergo for a proper education and training. Process Model of educational and training of security awareness on mobile device has been designed to guide ICT units to conducting the program. By implementing the course or program more or less will increase the student's security knowledge to be more aware to secure their device from any unauthorized access.

ABSTRAK

Teknologi semasa pesat berkembang untuk lebih maju. Dalam teknologi peranti mudah alih, semenjak ia telah menjadi sebahagian penting dalam kehidupan manusia seharian, pemaju berlumba-lumba menaik taraf peranti mudah alih kepada prestasi yang lebih baik. Telefon pintar (Smartphone) telah menggantikan telefon bimbit dan ia telah digunakan secara meluas disebabkan oleh kemajuan teknologi yang ditawarkan. Memiliki sepenuhnya fungsi seakan-akan dan ciri-ciri telefon pintar dengan komputer membuat peranti tersebut lebih terdedah kepada pelbagai ancaman keselamatan seperti "*Malicios Code*" (termasuk juga *"virus"*, *"worm"* dan *"trojan"*) dan beberapa kelemahan yang lain. Pelajar sering kali taksub dalam mempunyai teknologi yang canggih akan tetapi kebiasaannya tahap kesedaran mereka amatlah kurang terhadap peranti mudah alih yang dimiliki. Kekurangan pendidikan keselamatan dan berasakan peranti mereka sudah cukup selamat menyebabkan para pelajar mengabaikan dalam menggunakan ciri-ciri keselamatan kepada peranti mudah alih. Oleh kerana itu, kajian ini telah dijalankan kepada pelajar UTM dengan mengedarkan soalan pra-kajian bagi mengenal pasti keadaan semasa tahap kesedaran dan pengetahuan teknologi berkaitan. Keputusan didapati bahawa mereka masih berada pada tahap kesedaran yang rendah dan seharusnya mereka perlu untuk menjalani pendidikan dan latihan yang sepatutnya. Proses model pendidikan dan latihan kesedaran keselamatan pada peranti mudah alih telah digubal untuk dijadikan panduan kepada unit ICT untuk menjalankan program tersebut kepada pelajar. Dengan melaksanakan program kursus, sedikit sebanyak akan meningkatkan kadar pengetahuan keselamatan pelajar untuk menjadikan mereka lebih berhati-hati dalam mengelakkan peranti mudah alih mereka daripada diakses tanpa kebenaran.

TABLE OF CONTENT

LIST OF TABLE

LIST OF FIGURE

LIST OF ABBREVIATION

GPS	Global Positioning System
ICT	Information Communications Technology
IM	Instant Messaging
IS	Information System
IT	Information Technology
LAN	Local Area Network
MMS	Multimedia Messaging Service
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
SMS	Short Message Service
UTM	Universiti Teknologi Malaysia

LIST OF APPENDIX

CHAPTER 1

INTRODUCTION

1.1 Introduction

The word “security” towards people will appoint with something that related to a degree of protection against the danger, damage, loss, harm and crime. Security becomes a form of protection structures and processes that provide to improve the security mechanism as its condition. Besides, every work that we are on will require a security and safety. *“Safety First”* is the most common message on signboard that been placed at the construction sites and workstation which highly expose to death risk. This alone shows us that the security issues are crucial as fatal injury and big loss will take place whenever people being insignificant during their duty.

Since Information Technology is in high demand technology and widely used by human being in this century, security issues in this area also rapidly increase as current issue happened which mentioned in online media web “Utusan Malaysia date on 24 Jun 2011”. In that article, Vice President Cyber Security Responsive Service; Adli Abd Wahid said, mostly the internet user in Malaysia doesn’t know a right way to secure their computer and their data. Furthermore, they not even alert or know what actually firewall work is for. He advised to all users should learn security education (IT) to prevent security breaches that happened to Malaysian Government Websites on the date before.

Security awareness is important and a must needs to any organization. Information security management is terms of technical and procedural controls that protect information assets with respect to confidentiality, integrity and availability. However, many of these controls miss their effectiveness when staff/employees act in a security-negative manner which refer to, they do not aware the risk of their current insecure behavior and they set aside the organization’s policy and standards because it is more convenient to work like that. Hence, by implementing effective security will depend on creating an information security-positive environment, which the staff/employees understand and act accordingly to behave supposedly.

1.2 Problem Background

Mobile devices nowadays are widely used by all human beings in the entire world. Its revolution has been updated year by year to satisfy a good services and application to human life. Mobile device makes human life at ease level as everything is just under the user’s fingertip. As simple as one click button will show all the information needed instantly. Besides, with a thousand of applications that provided by the function of each device which collaborate with the provider of the service, for example, people can manage to pay a bill, to transfer an amount, to book a flight ticket and even can manage or view their share market just by using their mobile device.

Mobile devices such as cellular phone, PDA (Personal Digital Assistant), Smartphone and Tablet PC are exposed to various security threats like malicious code which included virus, worm and Trojan horses), vulnerabilities of mobile device, attacks on network communication, data or information robbery and damage also a mobile spam (Kim and Leem, 2005).

With rising up amount of information being sent and communicate through wireless channels, new threats also increase. Later, information security will become a critical issues to mobile devices and be a great concern to mobile devices users, just like what computer users do today (Bouwman, et al., 2006; Malloy, et al., 2002).

It has been realized that information is not just a technology problem, and in a recent years it becomes a hot topic to study the human factors in information security in the field of cyberspace (Hassel and Wiedenbeck, 2004; McCauley-Bell and Crumpton, 1998; Proctor et al., 2000). Since security issues related to mobile devices are different from that which related to computer. As example, mobile device might be infected with virus through the instant messages; users conducting mobile commerce may perceive security also differently from conduct e-commerce through computers or laptop; and personal privacy related to mobile devices also different.

Till now, security and privacy awareness of mobile internet usage has drawn few attentions in research and industry (Maurer, 2010). With the raise number of users that employ those devices for security sensitive tasks like internet banking, therefore security and privacy mechanism for mobile devices should be considered in the future.

1.3 Problem Statement

Many organizations have work hard to protect their asset from any harm, damage, loss, stealing, etc. Some of them have spent over thousand to have such strong security mechanism to protect their belongings. By installing a good security mechanism is not enough while security awareness among the employee/staff still at low level. The intruders may use social engineering in order to get pass through the security tools which been applied. Even some of professional also does not aware at all in their action in working.

Awareness often overlooked neither organization nor people around the world. They mostly are focusing on having an advance technology and depending on expert to monitor the security issues while information security awareness is the root state whereby people will aware on their security mission (Siponen, 2000).

In this study, the problem statements have been identified. Usually students are obsessed to advance technology such as smartphone or others pocket size gadget whereby it was providing a multiple and various functions that complement with the requirement in their life style. Besides, as mentioned by (Androulidakis, 2010) the security of mobile devices is proven not to be sufficient enough in many research papers. The advance and modern mobile devices, specifically smartphones are vulnerable to various security risks.

By adopting the mobile devices without any security knowledge or lack of awareness concern by thinking that the device is secure enough will lead the students being exposed to those mobile device vulnerabilities and risk. This may harm their devices and personal information might be stolen. Therefore information security education should become a priority to be implemented to educational institution like United State was done in a past few year (Hentea, 2005). In addition, the researcher also stated that there are some aspects of security education model need a few attentions or make a review for changes.

Here are the lists of problems question that needs to be concern in doing this study, define as below:

i. Which level of student most at high-risk for security threat and lack of awareness?

ii. Does security awareness education course and training program should be held in University?

iii. Which aspects of current existing model that require some customization or modification?

iv. How does the propose model can increase the awareness among the students?

1.4 Project Aim

The aims of this study are to identify the current stage of awareness among the different level of student and their field either at low level, intermediate or high level and to propose a design of security awareness model that suit to UTM campus student's. Anyhow in order to raise up the security awareness concern between the organization and the student which can motivate them to alert or aware any of vulnerabilities and attack from any invader that may harm such an important or valuable data or information which can cause damage or loss toward the organization or individually.

1.5 Objectives

In this project, there are three objectives that need to be achieved in this project. There are as follows:

i. To identify current state of security awareness on mobile device user (UTM's student) before and after undergoes training or has a proper education in Security Awareness Course or Program.

ii. To design an appropriate model of Information Security Awareness to raise up awareness concern among students

iii. To validate the model which been proposed and analyze the validation result.

1.6 Project Scope

Scope of the project includes as the following areas:

i. The study focus on UTM campus as a target organization.

ii. The students of UTMs' are the target respondents.

iii. Survey will be done to a different faculty and different level of respondents.
iv. Survey result will signify the current stage of awareness concern among the mobile device user.
v. Generate the data and design the appropriate model to the ICT unit of UTMs' as a guideline to implement educational course or training program to students.

1.7 Significance of the Project

Significance of doing this study is mainly to suggest for the organization to follow the model that will be suggest. Security education and awareness program are crucial although by combining both would take a lot of time and energy. Experts generally agreed that people are the most common greatest source of IT security problems. Statistics consistently show that the majority of security breaches are caused by insiders, and the damage they levy on their organizations can be much more severe than anything wrought by hackers on the other side of the world (J.Pescatore, 2002).

Many, if not most, insider breaches are caused neither by disgruntled employees nor by students intent on doing harm. The sources are often as follows reason:

i. People are not aware of the security threats.
ii. People are wrongly relying on someone else to deal with them.
iii. People are not adequately skilled to address them.
iv. People simply feel they have more important things to do and neglect to aware those things.

1.8 Report Organization

This project study consists of four chapters in project 1. Every chapter is organizes accordingly to a different work that involved in the study. The detailed organization of this report is described in the following section of paragraphs:

Chapter 1 of this report consists overview of the study, problem background of the project, problem statement, objectives of the project, scope of the project and significance of this study.

Chapter 2 of this report covers recent review of the literature review that related to the study area which is information security, security awareness and mobile device that relate to each topic. Its will discuss the previous researcher work in scope security issues and its problem.

Chapter 3 explain the technique of method that to be use in the study and also operational framework been describe in details phase by phase that will represent the flow of all task in doing the study.

Chapter 4 is discussing on design implementation process. It's consist the processes on how the elements and the features been selected in order to developing the propose design model. Besides, matrix table also been map to each other to build a relationship to be a strong support for model design.

Chapter 5 will discuss on analysis and the result of the finding from the student's survey feedback. The result of the validation process of the model also explained as to be the finalized result of the design model.

Chapter 6 is the final chapter which consists of discussion on conclusion to the project. It does discuss on research achievement, challenge and constraint of doing the research and future recommendation towards the study. Lastly summarization of the research project will all conclude in this chapter.

REFERENCE

Adam Marks, Yacine Rezgui. *A comparative Study of Information Security Awareness in Higher Edecation Based on the Concept of Design Theorizing*. Journal.

Anind K.Dey, Jonna Hakkila (2008). *Chapter XIII*, *Context-Awareness and Mobile Device.* IGI Global Journal.

Anthony S.PARK, Steffen LIPPERTS, and Marc WILHELM (2001). *Location Based Services for Context Awareness-Moving from GSM to UMTS.*

Australian Government, Department of Broadband (2010). *National Cyber Security Awareness Awareness Raising and Educational Initiatives.* Research Report, May 2011.

Australian Communications and Media Authority (ACMA),. *An Overview of International Cyber Security Awareness Week.* Article 6-11 June 2010.

Berith L. Andersen, Martin L. Jorgensen, Ulrik Kold, Mikael B. Skov (2006). *iSocialize: Investigating Awareness Cues for a Mobile Socal Awareness Application*. Journal

Chao Li, Katharine Willis. *Modeling Contect Aware Interaction for Wayfinding using Mobile Devices.* Journal

Dirk De Maeyer. *Setting up an Effective Information Security Awareness Programme*. KPMG Advisory

E. Eugene Schultz (2007). *Risk due to Convergence of Physical Security Systems and Information Technology Environment.* Information Security Technical Report 12 (2007) 80-84.

E. Kritzinger, S.H von Solms (2010). *Cyber Security for Home User: A new way of Protection Through Awareness Enforcement.* Computer & Security 29 (2010) 840-847.

Fadi Aloul (2010). *The Need for Effective information Security Awareness*. Department of Computer Science & Engineering American University of Sharjah.

Frank Breitinger, Claudia Nickel (2010). *User Survey on Phone Security and Usage*. Publish paper.

Gaborone, Bostwana (May 2011). *Proceeding of the First IFIP TC9/TC11 Southern African Cyber Security Awareness Workshop 2011*. Workshop.

HA Kruger, L Drevin, T Steyn. *A Framework for Evaluating ICT Security Awareness*. Journal

Hyeonkoo Cho, Jungchan Na (2011). *Security Situation Awareness and Situation Information Generation Based on Spatial Linkage of Physical and IT Security*. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011.

Iosif Androulidakis, Gorazd Kandus. *Differences in Users' State of Awareness and Practices Regarding Mobile Phone Security Among EU Countreis*. Journal

Jason Gonzalez and James Hung, Stroz Friedberg LLC (2011). *Mobile Device Forensic: A Brave New World?*. Bloomberg Law Report.

L. Drevin, H.A. Kruger, T. Steyn (2007). *Value-Focused Assessment of ICT Security Awareness in an Academic Environment.* Computer & Security 26 (2007) 36-43

Liu Ying, Huang Dinglong, Zhu Haiyi, Patrick Rau. *Users' Perception of Mobile Information Security*. Journal

Mariana Hentea, *APerspective on Achieving Information Security Awareness.* Issue in Informing Science and Information Technology.

Max-Emanuel Maurer (2010). *Bringging Effective Security Warning to Mobile Browsing*. Journl

Mikko Hypponen (2006). *Malware goes Mobile.* Copyright 2006 Scientific American, INC article.

Mohammed Boujettif, Yongge Wang. *Constructivist Appproach to Information Security Awareness in The Middle East*. Journal.

Mollie K.Anderson (2008). *State of Lowa Enterprise Mobile Device Security Standard*. 5.19.2008

Muhammad Rabiul Hasan, Husnayati Hussin (2008). *Self Awareness before Social Networking: Exploring the User Behavior and Infromation Security Vulnerability in Malaysia*. Journal project

NIST-SP800-50. *Building an Information Technology Security Awareness and Training Progra.*

Retrieved from: *“https://www.mylookout.com/_downloads/lookout-mobile-threat-report-2011.pdf”*. June 2011.

Retrieved from: *“http://www.securityresearch.at/en/audit-services/awareness/”*. July 2012.

Retrieved from: *“http://www.nisc.go.jp/security-site/eng/about.html”*. July 2012.

Retrieved from: *“http://www.noticebored.com/html/why_awareness_.html”*. July 2012.

Retrieved from: *“http://www.securingthehuman.org/blog/2012/05/22/security-awareness-maturity-model/”*. May 2012.

Retrieved from: *“http://blog.afewguyscoding.com/2011/12/survey-mobile-device-security-threats-vulnerabilities-defenses/”*. Dec 2011.

Retrieved from: *“http://www.enterpriseitnews.com.my/component/k2/item/443-symantec-on-top-threats-targeting-mobile-devices.html”*. Dec 2011.

SANS Institute (2005). *Building a Security Policy Framework for a Large, Multi-National Company*. InfoSec Reading Room.

Shamsul Kamal Wan Fakeh, et al. (2012). *Information Security Awareness Amongst Academic Librarians.* Journal of Applied Sciences Reserach.

Shirley Payne (2003). *Developing Security Education and Awareness Programs*. Education Quarterly.

Theo Kanter (2003). *Cooperative Mobile Ambient Awareness*. Submission to MobEA workshop of the WWW2003 conference.

Yacine Rezgui, Adam Marks (2008). *Information Security Awareness in Higher Education: An Exploratoty Study*. Computer & Security 27 (2008) 241-253

Yiwei Cao. *Mobile Social Software with Context Awareness and Data Uncertainty for Technology-Enhanced Learning*. Journal