AN ANALYSIS ON SECURITY AWARENESS OF SOCIAL NETWORKS USERS

MAHDI DARVISHI

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 Computing
Universiti Teknologi Malaysia

JANUARY 2013

This project is dedicated to my beloved family and friends, without their Understanding, supports, and most of all love, the completion of this work would not have been possible.

ACKNOWLEDGEMENT

I wish to express my deepest appreciation to all those who helped me, in one way or another, to complete this project. First and foremost I thank God almighty who provided me with strength, direction and purpose throughout the project. Special thanks to my project supervisor Dr. Imran Ghani for all her patience, guidance and support during the execution of this project. Through his expert guidance, I was able to overcome all the obstacles that I encountered in these enduring ten months of my project. In fact, he always gave me immense hope every time I consulted with him over problems relating to my project.

ABSTRACT

Online social networking develops interactions and communication approaches. Online environment is the most beneficial approach for retention and inception of social relations. However, by developing facilities in online services the threats of privet security is increase. The information security vulnerability is an emerging problem in the online social networks social networks. The more users join, the more active they are, the more possible risk of personal information disclosure due to lack of self and social awareness on user behavior in the social networks. The main objective of the study is to investigate the components affecting information security behavior in enhancing awareness and design an information security behavior model in enhancing awareness. The quantitative research has been conducted on students studying at University Technology Malaysia. The study has found significant relationship between self-efficacy, security practice- care behavior, intention to practice privacy protection on information security awareness behavior. At the end, recommendations for future studies and limitations of the study were further established.

ABSTRAK

Rangkaian sosial dalam talian membangun interaksi dan pendekatan komunikasi. Persekitaran dalam talian adalah pendekatan yang paling bermanfaat untuk pengekalan dan permulaan hubungan sosial. Walau bagaimanapun, dengan membangunkan kemudahan perkhidmatan dalam talian ancaman keselamatan Privet peningkatan. Kegoyahan keselamatan maklumat adalah satu masalah yang muncul dalam rangkaian sosial dalam talian rangkaian sosial. Para pengguna lebih menyertai, lebih aktif mereka, risiko yang lebih kemungkinan pendedahan maklumat peribadi kerana kekurangan kesedaran diri dan sosial ke atas tingkah laku pengguna dalam rangkaian sosial. Objektif utama kajian ini adalah untuk menyiasat komponen yang mempengaruhi maklumat tingkah laku keselamatan dalam meningkatkan kesedaran dan reka bentuk keselamatan maklumat tingkah laku model dalam meningkatkan kesedaran. Penyelidikan kuantitatif telah dijalankan ke atas pelajar-pelajar yang belajar di Universiti Teknologi Malaysia. Kajian ini telah mendapati hubungan yang signifikan antara diri-keberkesanan, keselamatan amalan penjagaan tingkah laku, niat untuk mengamalkan perlindungan privasi atas tingkah laku kesedaran keselamatan maklumat. Pada akhir, cadangan untuk masa depan kajian dan batasan kajian telah terus ditubuhkan.

TABLE OF CONTENTS

LIST OF TABLES

LIS OF FIGURES

LIST OF ABBREVIATIONS

CSE	Computer Self Efficacy
DV	Dependent Variable
ISA	Information Security Awareness
ISSP	Information System Security Policy
IT	Information Technology
IV	Independent Variable
KMO	Kaiser Meyer Olkin
PBT	Protection Behaviour Theory
PMT	Protection Motivation Theory
SE	Self Efficacy
SEIS	Self Efficacy in Information Security
SPSS	Statistical Package for the Social Science

LIST OF APPENDICE

CHAPTER 1

INTRODUCTION

1.1 Introduction

In the recent years, social networking sites became a commonplace where people meet, discuss and share information among their friends and associates virtually. In the last few years, online communities have achieved an amazingly large audience. In the year 2007, researchers have found that 59 % of young adults, and 87 % of students are members and active users of the social networks (Schrammel *et al*., 2009). As the use of social networks became more widespread (Wu *et al*., 2010) thus, there are many studies have been conducted to understand the users' engagement and their online behavior in the social networks.

The information security vulnerability is an emerging problem in the online social networks social networks. The more users join, the more active they are, the more possible risk of personal information disclosure due to lack of self and social awareness on user behavior in the social networks.

1.2 Background of Problem

In the past few years, the popularity of social-networking websites such as Twitter and Facebook are increased. These social networks have a large number of end-users and large amount of information, by considering this issue; these websites have become a good target for attackers. However, these social networks try to reduce the impact of exploitations that are created by attackers; many attackers can launch more sophisticated attacks by using different attacks. By considering that threats are more sophisticated, it is obvious most of the users are not aware of these threats.

The problem is that the private information is shared by most social network users. There are some kinds of personal information that are shared by users such as contact information, images, demographic information, videos, comments, etc. Unfortunately, a large number of users publish their information without and considerations and this problem leads social network to become a big sensitive data loggers. Furthermore, social network users interest to rely on other social network users by accepting their friend requests and sharing personal items.

1.3 Problem Statement

Due to the rapid growth in popularity of the social networking sites such as Myspace and Facebook, information security issues have arisen because of the personal information disclosure in the various social networks, which could probably be misused by the computer criminals for identity theft or impersonation. However, with the high vulnerability of information security, the social networking sites remain as an open platform to communicate with one another. Many users today are not so serious about their personal data and information, which perhaps are disclosed in such social networks and many of them are less aware of the consequences of revealing the sensitive information during the communication in the social

networking sites. With realizing this issue of security dilemma, this research inspects the necessity of creating user-awareness before and after joining the social networks.

1.4 Research Questions

This research aims to answer the following questions:

What are the impacts of privacy policy (PP), Self-efficacy (SE), Security practice care behavior (SPCB), Intention to practice privacy protection and Security practice technology (SPT) on information security awareness?

i. How to implement a model for improving user security awareness?

1.5 Research Objectives

This research aims to answer the following questions:

i. To measure the impacts of the privacy policy (PP), Self-efficacy (SE), Security practice care behavior (SPCB) , Intention to practice privacy protection and Security practice technology (SPT) on information security awareness
ii. To propose a security awareness model.
iii. To test and validate the model.

1.6 Scope and Limitations

This work intends to explore why security unawareness may lead to the information security vulnerably. This study inspects the necessity of creating user-awareness for the social networks, and also examines the user behavior in that networks particularly in the context of UTM university in order to find out whether those users are aware of their activities in such social networks. The methodology of the study mainly involves a quantitative survey framework for data collection of the Facebook users.

1.7 Significance of the Proposed Work

Human factors play a significant role in computer security, which almost certainly influences other factors also. Since human resource contributes to security threats and vulnerability, technical consideration alone for security approaches to computer systems is inadequate. Good user security awareness program can reduce security risk significantly and prevent systemic financial losses which are incurred annually as a result of lack of human resources knowledge in respect of security awareness.

The significance of self awareness in social networking is very much high in the era of information superhighway. There are many incidents happened in terms of online privacy and security in various social networking sites around the globe. With realizing this issue of security dilemma, this research inspects the necessity of creating user-awareness before and after joining the social networks.

1.8 Organization of the Research

The organization of this thesis is as follows: Chapter 1 presents a general discussion on the topic of the thesis and the issues that need to be solved by introducing statement of problems, set of objectives, and the scopes of research. The related available literatures are reviewed and discussed to achieve the necessary knowledge for developing the research objectives is in Chapter 2. Chapter 3 discusses the research methodology that is employed to achieve the objectives of this research. Chapter 4 discusses the proposed framework

to assess the level of information security awareness for social network (facebook). Chapter 5 discusses result of study. Finally, conclusion and recommendation discuss in chapter six.

REFERENCES

Adams, A., Sasse, M.A., and Lunt, P. (1997). Making passwords secure andusable. People and Computers, 1-20.

Alavi, M & Leidner, D.E 1999, Knowledge management system s: issues, challenges, and benefits, Communications of the AIS, 1(2es).

Anderson, C. L., Agarwal, R. (2010). Practicing safe computing: a multimedia

empirical examination of home computer user security behavioral intentions. Mis Quarterly. 34(3), 613-643.

Arora, A., D. Hall, et al. (2004). "Measuring the risk-based value of IT security solutions." IT Professional 6(6): 35-42.

Bandura, A. (1997). toward a unifying theory of behavioral change. P sychological review. 84(2), 191.

Bandura, A(1991). Social cognitive theory of self-regulation. Organizational Behaviour and Human Decision Processes.

Boyd D.(2004). Friendster and publicly articulated social networking .in the Proceeding of Conference on Human Factors and Computing Systems.

Brace, I. (2008). Questionnaire design: How to plan, structure and write survey material for effective market research, Kogan Page Ltd.

Bryman, A., and Becker, S. (2008). Quality criteria for quantitative, qualitative an mixed methods research: The view from social policy, International Journal of Social Research Methodology.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly.84(4), 415-643.

Cavusoglu, H., Mishra, B., and Raghunathan S. (2004). A model for evaluating IT security investments. Communications of the ACM. 47(7), 87-92.

Carpenter, J., et al. (2001). Continuing Threats to Home Users. CERT Advisory CA-2001-20.

Chan, M. Woon., and Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. Journal of information privacy and security. 1(3), 18-41.

Compeau, D. R., and Higgins, C. A. (1995). Computer self-efficacy: development of a measure and initial test. MIS Quarterly.

Goettke R. and Christiana J.(2007). Privacy and Online Social Networking Websites.

Govani, T., and Pashley, H.(2005) Student Awareness of the Privacy Implications whileUsing Facebook.

Exploitation—Social Networks Malware, ISACA Journal,http://www.rkmingenieria.com/ifol/wpcontent/uploads/2011/03/ISACA_JAN_2011_ChainExploitation.pdf

Cranor L., Gudruru P. and Arjula M. (2006). User Interfaces for Privacy Agents. ACM Transactions on Computer-Human Interaction, Vol. 13, No. 2, June pp.135- 178.

Gross, R. and Acquisti. (2005). Information Revelation and Privacy in Online Social Networks(The Facebook case), in the Proceedings of the 2005 ACM workshop on Privacy in the electronic society. pp. 71 – 80.

G. Hogben. Security Issues and Recommendations for Online Social Networks. Position paper, ENISA, European Network and Information Security Agency, Octoeu/doc/pdf/deliverables/enisa_ppsocial_networks.pdf.

Herath, T., and Rao, H. R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems. 18(2), 106-125.

Herath, T., and Rao, HR. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems. 47(2), 154-165.

Hyeun, S., Cheongtag, K., and Young, U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. computers and security. 28(8), 816-826.

Ifinedo, P. (2011). An exploratory study of the relationships between selected contextual factors and information security concerns in global financial services institutions. Journal of Information Security and Privacy.

Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions: is national culture a differentiator? Information Management and Computer Security.

Jagatic, T. Social phishing. In Communications of the ACM Forthcoming (2006), 2006. www.indiana.edu/\~phishing/ social-network-experiment/ phishing-preprint.pdf.

Jankowicz, A. (2002). Business Research Projects, 3rd Edition, Thomson Learning, London.

Jonhston, A. C., and Warkentin, M. (2010). Fear appeals and information security behaviours: an empirical study. MIS Quarterly.

Kaiser, H. F. (1974). An index of factorial simplicity. Psychometrika.

Kamakura, W. A., and Russell, G. J. (1993). Measuring brand value with scanner data.

Kankanhalli, A., Tan, B. C. Y., and Wei, K. K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. Mis Quarterly.

Knapp, K. J., and Marshall, T. E. (2006). Information security: management's effect on culture and policy. Information Management and Computer Security.

Kosta, E. and Dumortier, J.(2008). Searching the man behind the tag: privacy implications of RFID technology. International Journal of Intellectual Property Management(IJIPM), Special Issue on: "Identity, Privacy and New Technologies".

Kotulic, A. G., and Clark, J. G. (2004). Why there aren't more information security research studies. Information and Management.

Kondakci, S. (2007). The First Step in Improving Security Awareness: A Simple Self-assessment Framework information security & cryptog rafycon ferance with international participation. turkey.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(03), 607.

L. Wu, M. Majedi, K. Ghazinour and K. Barker, "Analysis of social networking privacy policies" in Proceedings of the 2010 EDBTI1CDTWorkshops. 20lO, Switzerland.

Larose, R., and Rifon ,N. J. Enbody, R. (2008). Promoting personal responsibility for internet safety. Communications of the ACM.

Lee, Y., and Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. Communications of the ACM.

Lee, Y., and Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems.

Leonard, L., Cronan, T. P., and Kreie, J. (2004). What influences IT ethical behaviour intentions-planned behaviour, reasoned action, perceived importance, or individual characteristics? Information and Management.

Mackenzie, A. (2006). Cutting Code: Software and Sociality (New York: Peter Lan).

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. Information Systems Research. 2(3), 173-191.

Marakas, G., Johnson, R., and Paul F. (2007) The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time., Journal of the Association for Information Systems.

Martins, A., and Eloff, J. (2003). Information Security Culture, Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egypt. IFIP Conference Proceedings.

Milne, S., Sheeran., and P. Orbell, S.(2000). Prediction and intervention in health-related behaviour: a meta-analytic of protection motivation theory. Journal of Applied Social Psychology.

Marakas, G., Johnson, R., and Paul F. (2007) The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time., Journal of the Association for Information Systems.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems.

Ng ,B.Y., Kankanhalli, A., and Xu YC. (2009). Studying users' computer security behaviour: a health belief perspective. Decision Support Systems.

Ng, B. Y., and Rahim, M. A. (2005). A socio-behavioral study of home computer users' intention to practice security 7-10.

Oppenheim, A. (1992). Questionnaire Design, Interviewing and Attitude Measurement, London, Pinter.

Ozer, E., and Bandura, A. (1990). Mechanisms governing empowerment effects: A self-efficacy analysis. Journal of Personality and Social Psychology.

Pahnila, S., Siponen, M., and Mahomood, A. (2007). Employees' behaviour towards IS security policy compliance. In: Proceedings of the 40th Hawaii International Conference on System Sciences, January 3e6, Los Alamitos, CA.

Pechmann, C., Zhao, G., Goldberg, M., and Reibling, E.T. (2003). What to convey in antismoking advertisements of adolescents: the use of protection motivation theory to identify effective message themes. Journal of Marketing.

Peterson , S. J., and Luthans, F. (2006). The impact of fi nancial and nonfi nancial incentives on business - unit outcomes over time . Journal of Applied Psychology.

Proctor, R.W and Proctor, J.D. (2006). Handbook of Human Factors and Ergonomics 3rd ed., John Wiley and Sons, New York.

Rabii, T. and K. Ward (2010). "Risky Business at Wireless Hot Spots ".

Rhodes, K. (2001). Operations security awareness: the mind has no firewall. Computer Security Journal.

Richardson, R. (2007). CSI Computer Crime and Security Survey. Computer Security Institute. From: retrieved November 16, 2007.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo and R. Petty ,Social Psychophysiology. New York: Guilford Press.

Sasse, M. A., Brostoff, S., and Weirich, D. (2004). Transforming the weakest link e a human/computer interaction approach to usable and effective security. BT Technology Journal.

Saunders, M., Lewis, P., and Thornhill, A. (2007). Research Methods for Business Students 3rd edition Harlow: Prentice Hall.

Schrammel, C. KotTel and M.Tscheligi, "Personality traits, usage patterns and information disclosure in online communities", in Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology. 2009, pp.169-174.

Sekaran, U. (2006). Research method for business, A skill building approach, New Delhi, John Whiles and Sons.

Sekaran, U. (2010). Research methods for business: A skill building approach. New York: John Wiley and Sons.

Skinner, E. A. (1995). Perceived control, motivation, and coping. Thousand Oaks, CA: Sage.

Siponen, M., and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly.

Stanton, J. M., Stam, K. R., and Jolton, J. (2005). Analysis of end user security behaviours. Computers and Security.

Stajkovic , A. D. , and Luthans , F. (1998). A meta - analysis of the effects of organizational behaviour modifi cation on task performance. Academy of Management Journal.

Tan, P. (2000). Business excellence in entrepreneurship through motivation audit. Managerial Auditing Journal.

Thomson, M., and Solms, R .(1998). The development of an erective information security awareness program for use in an organization. Unpublished master's thesis, Port Elizabeth Techniko.

Torkzadeh, G.,and VanDyke, T. P. (2001). Development and validation of an internet self-efficacy scale Behaviour and Information Technology.

Venkatesh,V., Morris, M., G.Davis, G. B., nad Davis,Fred D.(2003). User acceptance of information technology: Toward a unified view, MIS Quarterly.

Vroom C., and Solms, R. (2004). Towards information security behavioural compliance. Computers and Security.

Warkentin, M., and Willison, R. (2009). Behavioural and policy issues in information systems security: the insider threat. European Journal of Information Systems.

Whitten, A. (2004). Making Security Usable. Ph.D. Thesis. Unpublished PhD dissertation, Carnegie Mellon University.

Whitman, M.E. and Mattord, H.J. (2003). Principles of Information Security. Canada. Course Technology, 25 Thomson Place, Boston, Massachusetts.

Woon, I., Tan, G.,and Low, T. (2005). A protection motivation theory approaches to home wireless security. In: Avison D, Galletta D, DeGross JI, editors. Proceedings of the 26th International Conference on Information Systems, In Las Vegas, December P.

Woon, I., and Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications. International Journal of Human-Computer Studies.

Workman, M., Bommer, H. H., and Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. Computers in Human Behaviour.

wyer C., Hiltz R., and Passerini K.(2007).Trust and Privacy concern within social

networking sites: A comparison of Facebook and MySpace, in the Proceedings of AMCIS .

Zhang, Y., and Espinoza, S. (1998). Relationships among computer self-efficacy, attitudes toward computers, and desirability of learning computing skills. Journal of Research on Technology in Education.