UNIVERSITI PUTRA MALAYSIA

RISK AWARENESS MODEL FOR SECURITY AND PRIVACY IN SOCIAL NETWORKING SITES FROM THE USERS' PERSPECTIVE

BALOGUN KAMORU ABIODUN

FSKTM 2022 17

RISK AWARENESS MODEL FOR SECURITY AND PRIVACY IN SOCIAL NETWORKING SITES FROM THE USERS' PERSPECTIVE

By

BALOGUN KAMORU ABIODUN

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Doctor of Philosophy

July 2021

DEDICATIONS

This thesis is dedicated to my beloved

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Doctor of Philosophy

RISK AWARENESS MODEL FOR SECURITY AND PRIVACY IN SOCIAL NETWORKING SITES FROM THE USERS' PERSPECTIVE

By

BALOGUN KAMORU ABIODUN

July 2021

Chairperson : Azmi Bin Jaafar, PhD
Faculty : Computer Science and Information Technology

The ability to interact with other people has become one of the most popular web-traffic phenomena in the digital age. There are risks connected with the Social Networking sites, which provides the potential of having victims investigated in a variety of ways to assess and limit. There are several ways for a user to prevent or minimize the degree of danger for the Social Networking sites, such as ensuring that the computer and Social Networking Sites have adequate security measures in place and limiting unnecessary clicking of unauthorized links. Besides, users can request that their profile be erased when it becomes obsolete. Being cautious about the applications is also another method of minimizing risks associated with Social Networking sites. It is also important to generate unique passwords coupled with being cautious on social media to ensure that their actions are limited. Additionally, configuring and reviewing the Social Networking sites privacy policy regularly can offer appropriate protection. Many studies show that the more a person visits a website, the more likely they are to be targeted by risk associated with Social Networking Sites. A major contribution of the study is risk awareness model development and proposed Social Networking sites Risk Meter (SNSR).

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

MODEL KESEDARAN RISIKO UNTUK KESELAMATAN DAN PRIVASI DALAM LAMAN RANGKAIAN SOSIAL DARI PERSPEKTIF PENGGUNA

Oleh

BALOGUN KAMORU ABIODUN

Julai 2021

Pengerusi : Azmi Bin Jaafar, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Keupayaan untuk berinteraksi dengan orang lain telah menjadi salah satu fenomena trafik web yang paling popular dalam era digital kini. Terdapat risiko yang berkaitan dengan tapak Rangkaian Sosial, yang memberikan potensi untuk menyiasat mangsa dalam pelbagai cara untuk menilai dan menghadkan. Terdapat beberapa cara untuk pengguna menghalang atau meminimumkan tahap bahaya apabila menggunakan tapak Rangkaian Sosial, seperti memastikan komputer dan tapak Rangkaian Sosial itu mempunyai langkah keselamatan yang mencukupi serta menghadkan klik-klik yang tidak perlu pada pautan yang tidak diizinkan untuk pengguna. Selain itu, pengguna juga boleh meminta agar profil mereka dipadamkan apabila ianya sudah usang dan tidak digunakan lagi. Berhati-hati tentang aplikasi yang digunakan juga merupakan satu kaedah untuk meminimumkan risiko yang berkaitan dengan pengunaan tapak Rangkaian Sosial. Ia juga penting untuk menjana kata laluan yang unik dan digabungkan dengan berhati-hati di media sosial dengan memastikan tindakan mereka terhad. Sebagai tambahan, mengkonfigurasi dan menyemak dasar privasi sesuatu tapak Rangkaian Sosial dengan kerap boleh menawarkan perlindungan yang bersesuaian. Banyak kajian menunjukkan bahawa semakin banyak seseorang melawat tapak web, semakin besar kemungkinan mereka disasarkan oleh risiko yang dikaitkan dengan tapak Rangkaian Sosial. Sumbangan utama kajian ini ialah pembangunan model kesedaran risiko dan cadangan tapak Meter Risiko Tapak Rangkaian Sosial.

ACKNOWLEDGEMENTS

I wish to thank my supervisor Associate Professor Dr Azmi Bin Jaafar and my distinguished Supervising committee Associate Professor Dr Marzanah A Jabar, Associate Professor Masrah Azrifah Azmi Murad for the way in which they empowered me to do and complete my research. I am truly grateful for your support and guidance, thank you. My great appreciation is expressed to my families for the patience, love and support you gave me during my study. Your encouragement was a crucial motivating factor that helped me to finish this study.

I would like to express my deep thanks to my colleagues in Person of Abdul- majid Babangida Umar and Maaruf Lawal for their support during my PhD programme

I would like to extend my profound thanks to my colleagues at AIRG Group and AIRG laboratory mates for their support and understanding. Without your support, I would not have had the chance to complete my PhD. My spe- cial appreciation goes to my friends who truly supported and encouraged me during all stages of my research.

Special thanks to my wife Alhaja Jemilat Bukola Oyetoyan Balogun and to my Children and my Uncle Alhaji Imam Abdul Fatai Quadri, Finally, my thanks and praise is to Almighty Allah.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy**.** The members of the Supervisory Committee were as follows:

Azmi bin Jaafar, Ph.D
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Marzanah binti A. Jabar, Ph.D
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Masrah Azrifah binti Azmi Murad, Ph.D
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 19 May 2022

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: Balogun Abiodun Kamoru

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: Associate Professor Dr. Azmi Bin Jaafar

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Marzanah binti A. Jabar

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Masrah Azrifah binti Azmi Murad

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ATT	Attitude
AVE	Average Variance Explained
CB-SEM	Covariance Based Structural Equation Modeling
CIA	Confidentiality Integrity Availability
CMCO	Conditional Mobility Control Order
CR	Composite Reliability
CV	Convergent Validity
DV	Discriminant Validity
EV	Expert Validation
HTMT	Heterotrait Monotrait
I-CVI	Item-Level Content Validity Index
IDE	Integrated Development Environment
IU	Intention to Use
OS	Operating System
PE	Perceived Enjoyment
PEU	Perceived Ease of Use
PLS-SEM	Partial Least Square Structural Equation Modeling
PP	Perceived Privacy
PRAM	Proposed Risk Awareness Model
PS	Perceived Security
PT	Perceived Trust
PU	Perceived Usefulness
RAM	Risk Awareness Model
SN	Social Network

SNS	Social Networking Sites
SNSR	Social Networking Site Risk Level
SNSRM	Social Networking Site Risk Meter
SNST	Social Networking Site Theory
STERR	Standard Error
TAM	Technology Acceptance Model
TAT	Technology Acceptance Test
TEV	Theory of Expectancy Value
TPB	Theory of Planned Behaviour
TR	Trust
TRA	Theory of Reasoned Action
VIF	Variance Inflator Factor

CHAPTER 1

INTRODUCTION

1.1 Overview

Web (apps) applications have grown in popularity and acceptability as handy channels of information and service delivery across a wide range of disciplines since the early days of the dot com boom in the late 1990's. These apps have recently moved from being merely information access tools to becoming engagement tools, allowing for the finding and exchange of information, content, and views. As a result, social networking sites (SNS) have become a significant element of today's internet. Active social network providers make up about 3.96 billion of the 4.57 billion internet users, according to Data reportal's digital 2020 July worldwide statshot (Kemp, 2020). This corroborates the notion that user involvement in social networking sites has progressed from a "niche phenomenon" to "the maximum degree of widespread adoption" (Gupta and Dhami, 2015).

However, in the midst of this fast expansion, social media platforms have prompted worries about risk (Chena and Sharma, 2013). Users of social media sites are vulnerable to content manipulation, cyber harassment, malware, data theft, online stalking, spam, and phishing, according to Gupta and Dhami (2015), and may suffer reputational harm, monetary loss, or at the very least, emotional distress. Most people's personal information, for example, has been exposed to unidentified analysis. Individual harassment because of disclosing personal information, cyber bullying, and even identity theft are all instances of particular occurrences. A better risk-measuring methodology must take into account the consumers' perception of security and privacy risks. Consequently, research into social media danger situations and feasible usage rules is on the rise (Breward, 2007).

1.2 Problem Statement

The use of social networking platforms is influenced by privacy and security concerns. An attempt was made by Ashish and Anil (2015) to separate these two characteristics in order to better understand how information may be shared on social networking platforms. Transmitting and exchanging private information is all considered to be under the category of "privacy." Social networking programs have been portrayed as innocuous, on the other hand, when it comes to security (Breward, 2007).

However, existing research has not been able to relate users' behavior to the security and privacy concerns they face when utilizing social networking sites.

A recent study by Kusev and colleagues investigated the risk preferences of humans when it came to the use of certain technologies and occupations. To depict risk and its link to an individual's yearly income, they relied on a statis- tical measure of demise.

However, the technique used to evaluate users' preferences has a number of flaws, including changes in preferences over time, failure to account for the changeability of hazards, the underlying assumption that users have all information, and the presence of alternative risk-benefit metrics.

Users' risk perceptions of various social networking platforms and the activities they can do have been investigated using a variety of psychometric techniques. These techniques have been able to provide advantages in terms of eliciting users' risk perceptions as well as information on how the outcome affected their behaviour. This implies that risk communication and appropriate regulations might be the result of such scholarly effort utilizing these techniques (Zarouali et al., 2018; Trepte et al., 2015).

Alternative research has looked at the link between users' risk perceptions and their usage of social networking sites, as well as whether or not they are victims of online victimization. They discovered that there are a number of discrepancies in behavioural research performed on social networking sites, with the majority of them focusing on privacy concerns, while others are lacking security concerns (Memon et al., 2018).

Several studies on security and privacy on social media sites have revealed that there is still a study vacuum in the area of social media risk. Although recent studies have looked at the impact of SNS on businesses in a favorable light, the risk element has not been fully addressed. Practical concerns, such as users' perceptions of SNS security and privacy, their attitudes, and trust, have yet to be investigated. As a result, there is a need to investigate the relationship between SNS risk and users' perceptions of privacy, security, attitude, and trust (Damghanian et al., 2016).

The use of social networking platforms is influenced by privacy and security concerns. An attempt was made by Ashish and Anil (2015) to separate these two characteristics in order to better understand how information may be shared on social networking platforms. Transmitting and exchanging private information is all considered to be under the category of "privacy." Social networking programs have been portrayed as innocuous, on the other hand, when it comes to security (Breward, 2007).

However, existing research has not been able to relate users' behavior to the security and privacy concerns they face when utilizing social networking sites. A recent study by Kusev and colleagues investigated the risk preferences of humans when it came to the use of certain technologies and occupations. To depict risk and its link to an individual's yearly income, they relied on a statis- tical measure of demise.

However, the technique used to evaluate users' preferences has a number of flaws, including changes in preferences over time, failure to account for the changeability of hazards, the underlying assumption that users have all information, and the presence of alternative risk-benefit metrics.

Users' risk perceptions of various social networking platforms and the activities they can do have been investigated using a variety of psychometric techniques. These techniques have been able to provide advantages in terms of eliciting users' risk perceptions as well as information on how the outcome affected their behaviour. This implies that risk communication and appropriate regulations might be the result of such scholarly effort utilizing these techniques (Trepte et al., 2015; Zarouali et al., 2018).

Alternative research has looked at the link between users' risk perceptions and their usage of social networking sites, as well as whether or not they are victims of online victimization. They discovered that there are a number of discrepancies in behavioural research performed on social networking sites, with the majority of them focusing on privacy concerns, while others are lacking security concerns (Memon et al., 2018).

Several studies on security and privacy on social media sites have revealed that there is still a study vacuum in the area of social media risk. Although recent studies have looked at the impact of SNS on businesses in a favorable light, the risk element has not been fully addressed. Practical concerns, such as users' perceptions of SNS security and privacy, their attitudes, and trust, have yet to be investigated. As a result, there is a need to investigate the relationship between SNS risk and users' perceptions of privacy, security, attitude, and trust (Damghanian et al., 2016).

1.3 Research Questions

The preceding sections' discussions clearly show the necessity for study to aid in the knowledge of the hazards associated with social networking sites. This research is an attempt to do so (Hassan et al., 2006). The project will address the following research questions in order to achieve this goal:

i. What are the main dangers associated with the use of social media sites?

ii. What is the nature of the link between perceived security, perceived privacy, and the danger of using social media sites?

iii. What is the best way to investigate the link between perceived security, privacy, and social media risk?

1.4 Research Objectives

The main objective of this research is to develop a model for assessing/measuring security and privacy in social media.:

i. To develop risk awareness model in Social Networking Sites on users perspective.

ii. To proposed a social Networking sites risk level Meter called (SNSR).

iii. To test and validate the suggested risk-awareness model methodology in a real-world setting beyond social networking sites.

1.5 Research Scope

To achieve the main objective for this research work, it is imperative to identify major risk factors related to security and privacy of social media from existing studies. This research work placed more effort on such risk factors as perceived by users, not developers. The research also includes only risk factors that can be conceptualized into a realizable model. Technical factors of risk and privacy are therefore excluded from the study (Hassan et al., 2006).

1.6 Thesis Organization

This study is divided into six sections. The first chapter provides an overview of the phenomena under investigation, as well as the research topic, research questions, research goals, and a brief explanation of the study's scope.

In Chapter 2, a comprehensive survey of literature was undertaken to offer a solid theoretical underpinning to the notion and a demarcation of the investigation. This covers a discussion of the basic idea of social networking, dangers associated with SNS use, relevant theories that might guide the study, a review of similar studies on SNS risk, and a discussion of security and privacy in SNSs (Andrews et al., 2007).

The study technique was described in depth in Chapter 3. It is divided into six sections: I. literature review, II. model formulation, III. empirical research, IV. proposed model, V. prototype creation, and VI. model validation.

The suggested research model and hypotheses are addressed in Chapter 4.

In Chapter 5, a system prototype is used to demonstrate the implementation of the research model with a detailed description of the findings of the investigations. This ranges from demographic data statistics to descriptive statistics of the acquired data, PLS-SEM analysis of the data to verify our assumptions, and the prototype's technological acceptance test.

Finally, Chapter 6 summarizes and concludes the whole study project.

REFERENCES

Ajzen, I. (2006). Constructing a theory of planned behavior questionnaire. Ali, F., Rasoolimanesh, S. M., Sarstedt, M., Ringle, C. M., and Ryu, K. (2018).

An assessment of the use of partial least squares structural equation modeling (pls-sem) in hospitality research. *International Journal of Contemporary Hospitality Management*.

Ananthula, S., Abuzaghleh, O., Alla, N. B., Chaganti, S., Kaja, P., and Mogilineedi, D. (2015). Measuring privacy in online social networks. *International Journal of Security, Privacy and Trust Management*, 4(2):1–9.

Anderson, J. C. and Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin*, 103(3):411.

Andrews, D., Nonnecke, B., and Preece, J. (2007). Conducting research on the internet: Online survey design, development and implementation guide- lines.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*.

Beldad, A. D. (2015). Sharing to be sociable, posting to be popular: Factors influencing non-static personal information disclosure on facebook among young dutch users. *International journal of web-based communities*, 11(3-4):357– 374.

Bertot, J. C., Jaeger, P. T., and Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. *Government information quarterly*, 29(1):30–40.

Breward, M. (2007). Perceived privacy and perceived security and their effects on trust, risk, and user intentions. In *Eighth World Congress on the Management of eBusiness (WCMeB 2007)*, pp. 4–4. IEEE.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., and Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, 35(3):445–459.

Chena, R. and Sharma, S. K. (2013). Understanding member use of social net- working sites from a risk perspective. *Procedia Technology*, 9:331–339.

Corritore, C. L., Kracher, B., and Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International journal of human-computer studies*, 58(6):737–758.

Creswell, J. W. and Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Damghanian, H., Zarei, A., and Siahsarani Kojuri, M. A. (2016). Impact of perceived security on trust, perceived risk, and acceptance of online banking in Iran. *Journal of Internet Commerce*,15(3):214–238.

Deng, X., Bispo, C. B., and Zeng, Y.(2014). A reference model for privacy pro- tection in social networking service. *Journal of Integrated Design and Process Science*, 18(2):23–44.

Doherty, C., Lang, M., Deane, J., and Connor, R. (2019). Information disclosure on social networking sites: An exploratory survey of factors impacting user behaviour on Facebook. In *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications*, pp. 91–110. IGI Global.

Drennan, J., Sullivan, G., and Previte, J. (2006). Privacy, risk perception, and ex- pert online behavior: An exploratory study of household end users. *Journal of Organizational and End User Computing (JOEUC)*, 18(1):1–22.

Fishbein, M. and Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. *Philosophy and Rhetoric*, 10(2).

Garg, V.and Camp, J. (2012). End user perception of online risk under un- certainty. In *2012 45th Hawaii International Conference on System Sciences*, pp. 3278–3287. IEEE.

Gupta, A. and Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites. *Journal of Direct, Data and Digital Marketing Practice*, 17(1):43–53.

Hair Jr, J. F., Sarstedt, M., Hopkins, L., and Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (pls-sem): An emerging tool in business research. *European business review*.

Hassan, Z. A., Schattner, P., and Mazza, D. (2006). Doing a pilot study: why is it essential? *Malaysian family physician: the official journal of the Academy of Family Physicians of Malaysia*, 1(2-3):70.

Henseler, J., Ringle, C. M., and Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In *New challenges to inter- national marketing*. Emerald Group Publishing Limited.

Hiatt, D. and Choi, Y. B. (2016). Role of security in social networking. *International Journal of Advanced Computer Science and Applications*, 7(2):12–15.

Hua, G. (2008). An experimental investigation of online banking adoption in China.

Isaac, S. and Michael, W. B. (1995). *Handbook in research and evaluation: A col- lection of principles, methods, and strategies useful in the planning, design, and evaluation of studies in education and the behavioral sciences*. Edits publishers.

Kemp, S. (2020). Digital 2020: July global statshot. *Data Reportal Global Digital Insights*.

Kline, R. B. (2011). Convergence of structural equation modeling and multi- level modeling.

Kline, R. B. (2015). *Principles and practice of structural equation modeling*. Guilford publications.

Kuhl, J. (1982). The expectancy-value approach within the theory of social motivation: Elaborations, extensions, critique. *Expectations and actions*, pp. 125–160.

Lin, K.-Y. and Lu, H.-P. (2011). Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in human behavior*, 27(3):1152–1161.

Lynn, M. R. (1986). Determination and quantification of content validity. *Nursing research*.

Massoro, Z. Z. and Adewale, N. T. (2019). Influence of attitude, subjective norms and personal innovativeness on intention to use open access journals: a case of agricultural research institutes. *Library Philosophy and Practice*, pp. 1–13.

Memon, A. M., Sharma, S. G., Mohite, S. S., and Jain, S. (2018). The role of on- line social networking on deliberate self-harm and suicidality in adolescents: A systematized review of literature. *Indian journal of psychiatry*, 60(4):384.

Papacharissi, Z. (2010). *A networked self: Identity, community, and culture on social network sites*. Routledge.

Schneider, F. (1999). Trust in cyberspace Washington.

Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers*, 22(5):428–438.

Talib, O. (2014). *Research and Thesis: If Only I Had Known*. MPWS Rich Re- sources.

Trepte, S., Dienlin, T., and Reinecke, L. (2015). Influence of social support received in online and offline contexts on satisfaction with social support and satisfaction with life: A longitudinal study. *Media Psychology*, 18(1):74–105.

Tuunainen, V. K., Pitkänen, O., and Hovi, M. (2009). Users' awareness of privacy on online social networking sites-case Facebook. *Bled 2009 proceedings*, p. 42.

Uma, S. and Roger, B. (2003). Research methods for business: A skill building approach. book.

Williams, K., Boyd, A., Densten, S., Chin, R., Diamond, D., and Morgenthaler,

C. (2009). Social networking privacy behaviors and risks. *Seidenberg School of CSIS, Pace University, USA*.

Yin, R. K. (2013). Validity and generalization in future case study evaluations.

Evaluation, 19(3):321–332.

Yousafzai, S. Y., Pallister, J. G., and Foxall, G. R. (2003). A proposed model of e-trust for electronic banking. *Technovation*, 23(11):847–860.

Yun, G. W. and Trumbo, C. W. (2000). Comparative response to a survey executed by post, e-mail, & web form. *Journal of computer-mediated communication*, 6(1): JCMC613.

Zarouali, B., Van den Broeck, E., Walrave, M., and Poels, K. (2018). Predicting consumer responses to a chatbot on Facebook. *Cyberpsychology, Behavior, and Social Networking*, 21(8):491–497.