Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2022, 9(3):1-8**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Factors that Influence Students on their Security Behaviours

Aeishah Nur Suhaily, Khairul Mizan Taib, Shamsul Kamal Wan Fakeh

Master of Information System Management, Faculty Information Management, Universiti Teknologi Mara

Abstract According to the researchers, the goal of this study is to evaluate the elements that influence students' security behaviours, specifically the perceived severity of the threat, perceived self-efficacy, perceived response efficacy, and perceived response costs. It has lately come to the notice of the information systems literature that students' security-related behaviour is of particular concern. A large number of studies, on the other hand, have produced inconsistent and contradictory conclusions regarding the influence of a number of crucial factors. The goal of this quantitative research work is to explore both the motive for protection and the behaviour associated with security. A survey of 199 postgraduate students from the Faculty of Information Management at UiTM Puncak Perdana was conducted in order to validate the study model developed using SmartPLS. Not only do the findings reveal a statistically significant positive association between all independent variables and the dependent variable, but they also correspond to the phrases and concepts that will be used in future study. The findings of the research are discussed in this publication. The objective of this research is to explore the elements that influence students' security behaviours and to discuss additional security behaviours that can be used as a guideline in the future.

Keywords Security behaviour, protection motivation, information security

Introduction

Student life revolves around computers and the internet. There are a variety of exchanges that result in sensitive information being left on their computers and the Internet storage. Online collaborative work is done using Web 2.0 technologies and social networking sites to save personal information. Students, for example, visit websites, click on pages, and search for terms. Encouraging folks to use their data is becoming increasingly popular as Internet penetration increases and the amount of data created online grows exponentially. However, once data is released or stored on the web, it is possible for it to be manipulated. For this reason, students are particularly exposed to big cyber-attacks including hacking, malware dissemination and viruses. It is now more important than ever to include information security education in IT education. Participants in information security education programmes such as security education, training, and awareness initiatives may become more security conscious, according to Ng et al. (2009). To create effective educational programmes, one must first understand the factors influencing consumer security attitudes and behaviours. Ensuring kids have 21st-century skills, instructors face a new tendency. This includes mandated professional development in ICT or incorporating ICT into teaching approaches such as using information systems to report grades and behaviour in some situations. Using public computers, setting weak passwords, or enrolling in multiple websites at once puts educators at danger (Chou & Chen, 2013). To examine how college students' views and behaviours toward information security are influenced. Researchers like Woon, Tan, and Low (2005) and Workman, Bommer, and Straub (2005) have empirically evaluated proactive behaviour. A modified PMT was used in this study to better understand students' security-related behaviours. It will also look into security-related behaviour and motivation. This paper's last goal is to analyse the elements that influence the paper's goals.

Problem Statement

The Malaysian Communications and Multimedia Commission found that young adults in Malaysia are avid Internet users. The same poll found that over 62.5 percent of respondents were in college, 34.90 percent in high school, 2.40 percent in elementary school, and 0.20 percent in other schools. The data reveals that college students are more active online than elementary or secondary school pupils. According to Marketing Magazine (2011), the number of Malaysian young adults who use the Internet and spend time online is increasing. They are more vulnerable to cyber security threats as their Internet usage increases. This situation warrants a look at the security habits of Malaysian university students. Although Internet users' security is a major concern in Malaysia and globally, this study will just look at Malaysian university students' security. This is because Malaysians aged 16 to 24 are the most avid Internet users, and university students, aged 18 to 25, are in this age group. In January 2021, Malaysia had 27.43 million internet users, according to Kemp (2021). Malaysian internet users increased by 738 thousand (2.8%) between 2020 and 2021. In January 2021, Malaysia has an 84.2% internet penetration rate.

Over the previous two decades, educational institutions' technology security infrastructures have improved dramatically. University security, awareness, education, and training programmes have been implemented simultaneously, teaching staff and students the importance of information assurance and best practises for protecting personal and institutional data. It is clear from the few studies on college students' information security behaviour that there is a lack of training and compliance in these areas. Students frequently share passwords, ID numbers, credit card information, and financial data, and do not follow normal network security standards (Hajli & Lin, 2016; Hu, Hart, & Cooke, 2006). Despite the current surge in interest in cyber security, little is known about students' knowledge and training in the field. Government agencies, businesses, and non-profits have commissioned studies and surveys to assess employee awareness of and compliance with information security rules. This knowledge is crucial for computer users to prepare for, avoid, handle, and manage cyber-attacks. Recent surveys in the public, commercial, and non-profit sectors demonstrate that people lack the knowledge and training to avoid being targeted by cyber-attacks (Anderson & Agarwal, 2010; Meso et al., 2013).

Those pursuing higher degrees face extra security risks because much of their everyday communication and educational activities are online (Mensch & Wilkie, 2011). Academic demands are increasingly being met online, according to Devi and Roy (2012). According to Mohd Ayub et al. (2014), the majority of Internet users in Malaysia are aged 15 to 34, including university students. Rezgui et al. (2008) and Sheng et al. (2010) found that young adults (18-24) are more vulnerable to security threats. For three reasons, the researchers believe the current study is crucial to understanding higher education students' cyber security behaviours. As the country's greatest Internet users, the findings will help determine future steps for the government. As a result, the researcher must determine the factors influencing pupils' security.

Scope of study

The study will focus on Malaysian university students and how they perceive security. However, the study's unit analysis is unique. The study's context is students and their security behaviours. Aspects of security-related behaviour are examined, including perceived severity, reaction efficacy, self-efficacy, and response cost. Using the protection motivation theory (PMT) model, this study will examine the relationship between protection motivation and security-related behaviour, as well as whether descriptive characteristics influence protection motivation.

Related Previous Research

1. Security-related Behaviour

Security-related behaviour is a comprehensive security strategy that monitors all significant activities to identify and address deviations from regular behaviour patterns. As machine learning advances, this type of security management will become increasingly important in protecting computers at network edge locations. Behavioral security programmes work differently than typical security processes. They also monitor data streams, but compare their activity to a baseline of expected behaviour, looking for anomalies. Applied mathematics and machine learning are used to identify statistically noteworthy events and alert investigators. While an organisation may still have to pick between signature-based and anomaly-based network security, there are many intrusions detection and prevention systems that combine the best of both strategies.

2. Protection Motivation

Fear appeals spawned PMT. For example, verbal persuasion or observational learning are used to avoid a threat. "Perceived severity" is the sum of "perceived severity," "perceived vulnerability" (occurrence frequency), and "perceived impact" in PMT. The subject's "response efficacy" to an event will trigger their cognitive appraisal process, resulting in attitude changes and ultimately action. The cognitive appraisal process is described as a protection motive. Preference is given to cognitive appraisal and coping skills rather than terror or flight from the occurrence in PMT. Rogers improved the model (Maddux & Rogers, 1983). Using Bandura's social cognition theory, the researchers modified the PMT to include "self-efficacy" (1977). The perceived threat's intensity was interpreted as its seriousness. It was described as a person's judgement of the threat's likelihood. The recommended intervention's perceived efficacy reflected its effectiveness in reducing the threat. Self-efficacy is the belief in one's ability to perform particular behaviours. Perceived severity, vulnerability, reaction efficacy, and self-efficacy all contribute to the prevention or management of negative events.

3. Perceived severity

According to theory, adversity heightens people's sensibilities and motivates them to act. The perceived severity affects defensive security behaviour positively. Human behaviour plays a crucial part in information security and should be guided to prevent attacks. (Gangire et al. For example, Youn (2005) found perceived severity correlated with student intentions to protect personal data online. Yoon, Hwang, and Kim (2012) discovered the same association among graduate students as Mohamed and Ahmad (2012) found among undergraduates. In their research, Yoon et al. (2012) found a similar correlation between InfoSec activities and college students deleting suspicious emails. Taneja et al. (2014) found a positive severity related with college students adopting Facebook privacy settings. Hanus and Wu (2016) showed a weak association between desktop security behaviour and undergraduate academic success.

4. Perceived Response Efficacy

There is no evident link between effectiveness of a reply and a person's security behaviour. While Lwin et al. (2012), Yoon et al. (2012), and Hanus and Wu (2016) found no association between response efficacy and information security behaviour, Mohamed and Ahmad (2012) did. Using multiple regression analysis, Ng et al. (2009) found a favourable correlation between perceived benefits and email security behaviour. According to their questionnaire, perceived advantages are more closely associated to response efficacy than response efficacy. Consider the line "Exercising caution before opening email attachments helps prevent viruses from infecting my machine."

5. Perceived Self-efficacy

The main rationale for integrating self-efficacy is that persons with better self-efficacy in ICT are eager to use ICT and enhance relevant abilities. Rhee et al. (2009) discovered that students who graduated and believe they can save online data used security software and acted in a more security-conscious manner. They also want to strengthen the current ICT security. Both Hanus and Wu (2016) and Ng et al. (2009) found comparable results with working university students. Sangmi et al. (2009) also found a link between students' self-efficacy regarding privacy and their information-sharing behaviour in middle school. The ability to protect one's personal information has been linked to activities like not giving personal information to unknown websites or opening unknown email senders. According to Lwin et al. (2012) and Mohamed and Ahmad (2012), adolescent self-efficacy in online data protection was linked to overall online data protection behaviour. Yoon et al. (2012) claim a similar link exists for behaviours like deleting suspicious emails or sharing IDs and passwords.

6. Perceived Response Costs

The study revealed a link between response costs and information security measures, with greater response costs leading to faster malware removal and Facebook privacy changes (Taneja et al. 2014 and Yoon et al. 2012). The study indicated that perceived benefits offered in information exchange increased teen website visitors' readiness to disclose personal information. As an example. Concerns about social media and private data led Mohamed and Ahmad (2012) to find limited support for response prizes. The path of response costs was not supported by Ng et al. (2009)'s analysis of email-related security behaviour, nor by Hanus and Wu (2016)'s analysis of security software adoption behaviour.

Research Objective

In this study, students are the primary focus, as are their security behaviours and how they influence them. To be more specific, the research aims are listed as follows:

RO1: To examine the relationships between perceived severity, perceived response efficacy, perceived self-efficacy and perceived response cost toward security-related behaviour among students.

RO2: To measure variables that influence the security behaviour among students.

Theoretical Framework

A theoretical framework includes concepts, current theories, definitions, and references to relevant academic literature. An understanding of the theoretical framework is required to link the research paper subject to the larger fields of knowledge being explored. Rogers (1975) first proposed PMT to explain the effects of fear on health-related behaviours such as exercising, avoiding alcohol, and protecting oneself. To predict people's intentions in various dangerous situations, this theory has been extended to other fields of study. PMT is the cognitive assessment process that occurs when a threat is perceived. The process has two stages: threat assessment and coping assessment.

Quantitative research is a way of learning from a sample of people. Quantitative research uses data collected from observations or measurements to answer questions about the sample population. In terms of this aspect, which affects students' security behaviours, the researcher would follow the positivism paradigm and use a quantitative approach.

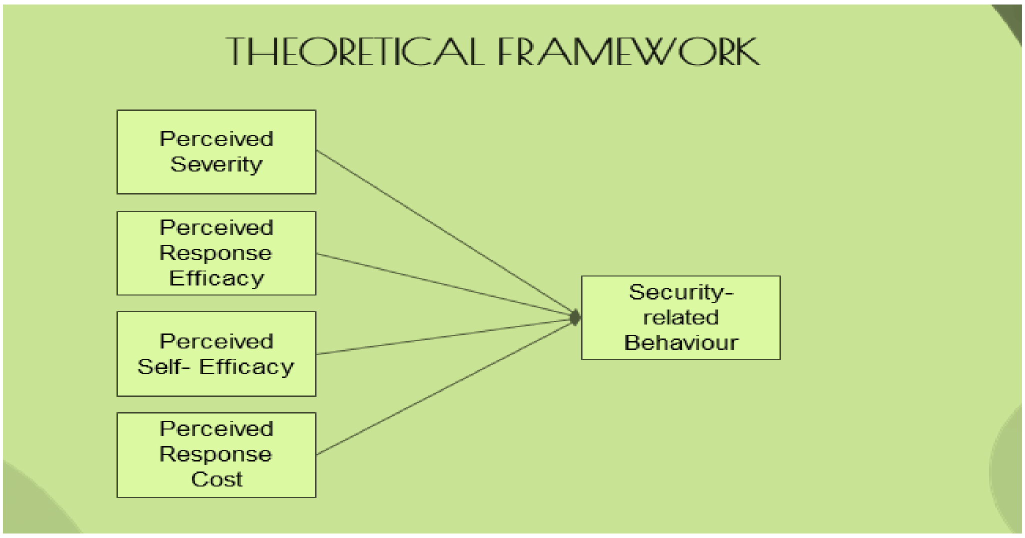

Figure 1: Theoretical Framework

This study will consist of Faculty of Information Management at UiTM Puncak Perdana.

Postgraduate students that use computers and have internet access within them. The sampling of this study will be conducted to 313 students of the Faculty of Information Management who need to answers completely the questionnaire has given. To achieve the sampling size target, the total number of questionnaires distributed will also answer the questionnaire using online survey distribution in Google Form. The scale of measurement used in this study is ordinal using Likert scales, and its application of statistical analysis is considered appropriate. The software that will be used is SmartPLS version 3 as software to key in data and analysis.

Data Analysis

A measurement model has satisfactory internal consistency reliability when the composite reliability (CR) of each construct exceeds the threshold value of 0.7. Table 1 shows that the CR of each construct for this study ranges from 0.824 to 0.889 and this is above the recommended threshold value of 0.7. Thus, the results indicate that the items used to represent the constructs have satisfactory internal consistency reliability.

Table 1 - Consistency reliability nd AVE value construct table

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Perceived Response Cost	0.803	0.855	0.863	0.611
Perceived Response Efficacy	0.743	0.749	0.853	0.660
Perceived Self- Efficacy	0.763	0.770	0.848	0.583
Perceived Severity	0.679	0.679	0.824	0.609
Security-related Behaviour	0.750	0.751	0.889	0.800

The measurement model's convergent validity is assessed by examining its average variance extracted (AVE) value. Convergent validity is adequate when constructs have an average variance extracted (AVE) value of at least 0.5 or more. Table 1 shows that all constructs have AVE ranging from 0.583 to 0.800, which exceeded the recommended threshold value of 0.5. This result shows that the study's measurement model has demonstrated an adequate convergent validity.

Indicator reliability of the measurement model is measured by examining the items loadings. A measurement model is said to have satisfactory indicator reliability when each item's loading is at least 0.7 and is significant at least at the level of 0.05. Based on the analysis, all items in the measurement model exhibited loadings exceeding 0.700; ranging from a lower bound of 0.736 to an upper bound of 0.900. All items are significant at the level of 0.001. Table 2 shows the loading for each item. Based on the results, all items used for this study have demonstrated satisfactory indicator reliability.

Table 2 - Indicator reliability

	Perceived Response Cost	Perceived Response Efficacy	Perceived Self-Efficacy	Perceived Severity	Security-related Behaviour
PS1				0.785	
PS3				0.765	
PS4				0.791	
RC1	0.796				
RC2	0.764				
RC3	0.796				
RC4	0.770				
RE1		0.815			
RE2		0.789			
RE4		0.833			
SB1					0.889
SB2					0.900
SE1			0.736		
SE2			0.797		
SE3			0.744		
SE5			0.775		

Each path connecting four latent variables in the structural model was a hypothesis. The structural model analysis allows the researcher to test each hypothesis and understand the strength of the relationship between dependent and independent variables.

It was used to examine the relationships between independent and dependent variables. However, Smart PLS generates t-statistics for all paths to test the significant level. The t-statistics output determines each relationship's significance level. This table lists all hypothesised paths' path coefficients, t-statistics, and significance levels. The proposed hypotheses are accepted or rejected based on the path assessment results. The next section discusses testing the hypotheses.

Table 3: Path Coefficients

	Original Sample (O)	**Sample Mean (M)**	**Standard Deviation (STDEV)**	**T Statistics (|O/STDEV|)**	**P Values**	**Hypothesis**
Perceived Response Cost -> Security-related Behaviour	0.033	0.043	0.067	0.495	0.621	Not Supported
Perceived Response Efficacy -> Security-related Behaviour	0.065	0.066	0.083	0.786	0.432	Not Supported
Perceived Self-Efficacy -> Security-related Behaviour	0.555	0.551	0.072	7.679	0.000	Supported
Perceived Severity -> Security-related Behaviour	0.041	0.048	0.064	0.630	0.529	Not Supported

Discussion and Results

Research Question 1: What are the relationships between perceived severity, perceived response efficacy, perceived self-efficacy and perceived response cost toward security-related behaviour among students?

In this study, the finding shows that there is a significance relationship between perceived severity, perceived response efficacy, perceived self-efficacy and perceived response cost and security-related behaviour (Rsquare= 0.380). Based on the results, it shows most the variable have a significant relationship with security-related behaviour. As for the questionnaire it confirms to be a good positive reliability and validity for the question as ranges from 0.824 to 0.889 and this is above the recommended threshold value of 0.7 and AVE ranging from 0.583 to 0.800. Additionally, the results indicate that cues to action, particularly institution efforts such as awareness programmes, are ineffective at motivating students to behave securely. This does not preclude the possibility of other types of action cues that were not quantified in this study. Again, the low correlation could be explained by the fact that the independent variable measures an organization's overall security efforts, whereas the dependent variable measures a student's specific security-related behaviour. It would be interesting to investigate whether the results would differ if cues to action quantified an institution's efforts to promote security-related behaviour.

Research Question 2: Which variables influence the security behaviour among students?

In this study only one of service quality dimension have been identified perceived self- efficacy to have positive influence on security behaviour among students except perceived response cost, perceived response efficacy and perceived severity. Perceived self-efficacy (β = 0.555, t = 7.679, p = 0.000)/ Perceived response cost (β = 0.033, t = 0.786, p = 0.621)/ Perceived response efficacy (β = 0.065, t = 0.786, p = 0.432)/ Perceived severity (β = 0.041, t = 0.630, p = 0.529) This study's findings are also consistent with those of previous studies. According to a study conducted by Rhee et al. (2009), students are capable of preserving online data and are not only employed on security protection software but are also engaged in security conscious behaviour when it is conducted more frequently. Concerning the others, Hanus and Wu (2016), as well as Ng et al. (2009), both reported similar findings regarding self-efficacy and security-related behaviour among students.

Regarding the other variables, such as perceived response cost, perceived response efficacy, and perceived severity, the hypotheses were rejected because they failed to demonstrate an influence on security-related behaviour. Taneja et al. (2014) and Yoon et al. (2012) discovered a negative correlation between perceived response costs and information security practises, indicating that students are more likely to delete malicious software and adjust their social media privacy settings. These variable lacks support in terms of the relationship between response costs and any security-related behaviour as mentioned in Ng et al. (2009) analysis.

Following that, there is no clear relationship between perceived response efficacy and security-related behaviour; the variable has a positive relationship (Hanus and Wu, 2016) between the independent and dependent variables, but there is no such relationship as Mohamed and Ahmad (2012) mentioned. As for the hypothesis, it is unsupported due to the fact that it is not directly influenced by security-related behaviour. The perceived severity hypothesis is not significant because it failed to demonstrate an association between the variable and students' security-related behaviour. Presumably, students are unaware of the severity of security incidents, and thus this variable has little influence on their security-related behaviour (Ng ang Xu, 2007). Additionally, the results indicate that a student's general interest in and predisposition toward security have no bearing on his or her security behaviour. Again, this could be because the benefits of security practise outweigh a student's individual security orientation. The correlation may be weaker because the items of general security orientation assess a student's general security orientation (towards general security practises), whereas the dependent variable assesses an individual's specific security-related behaviour.

Conclusion

The primary goal of this study is to identify and quantify student security-related factors. Within this framework, this article proposes a model for protection motivation theory. This paper will investigate the relationship between protection motivation and security-related behaviour in student computer use. The findings of this study are expected to be used to improve security-related behaviour among Malaysian students and to improve all factors influencing security behaviour. This study may inspire and persuade students to adopt safe computing practises. For example, the study's data collection method may help overcome some of its limitations. In a future study, the method of collecting feedback from respondents via a questionnaire could be expanded to include interviews, recording, observation, and other methods. Qualitative analysis can help researchers better understand security-related behaviour. This study could also be improved by adding variables related to security-related behaviour. There may also be additional potential influence drivers that have a greater impact on security-related behaviour. Finally, a larger sample size with a range of ages, educational backgrounds, and expertise can help generalise and potentially strengthen the findings among Malaysian students who use computers. Increasing the sample size and adjusting for educational background or experience may reveal new intentions, patterns, and computer behaviour. This study's limitations can be overcome by future research to obtain more detailed and accurate data on Malaysian students' privacy and security-related behaviour.

References

[1]. Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. MIS quarterly, 613-643.

[2]. Ayub, A. F. M., Hamid, W. H. W., & Nawawi, M. H. (2014). Use of Internet for Academic Purposes among Students in Malaysian Institutions of Higher Education. Turkish Online Journal of Educational Technology-TOJET, 13(1), 232-241.

[3]. Chou, H. L., & Chen, C. H. (2013). Exploration on high school teachers' perception of online personal data protection. Paper presented at the International Confer- ence of Taiwan Association for Educational Communications and Technology, Taipei, Taiwan. (in Chinese).

[4]. Devi, C. B., & Roy, N. R. (2012). Internet use among university students: a case study of Assam University Silchar. A journal of humanities and social science, 1(2), 183-202.

[5]. Featuring the Internet Usage Survey. (2011). Marketing Magazine

[6]. Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. Journal of Business Ethics, 133(1), 111-123.

[7]. Hu, Q., Hart, P., & Cooke, D. (2006, January). The role of external influences on organizational information security practices: An institutional perspective. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol. 6, pp. 127a-127a). IEEE.

[8]. Kemp, S. (2021, November 4). Digital in Malaysia: All the statistics you need in 2021 - DataReportal – global digital insights. DataReportal. Retrieved November 16, 2021, from https://datareportal.com/reports/digital-2021-malaysia

[9]. Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of experimental social psychology, 19(5), 469-479.

[10]. Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. Academy of Information and Management Sciences Journal, 14(2), 91-116.

[11]. Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. Journal of Information Privacy and Security, 9(1), 47-67.

[12]. Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Computers in Human Behavior, 28(6), 2366-2375. http://dx.doi.org/10.1016/ j.chb.2012.07.008.

[13]. Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815e825. http://dx.doi.org/10.1016/j.dss.2008.11.010.

[14]. Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computers & security, 27(7-8), 241-253.

[15]. Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting in- dividual's attitude and intention to use privacy controls on Facebook: An empirical investigation. Computers in Human Behavior, 38,159-173. http:// dx.doi.org/10.1016/j.chb.2014.05.027.

[16]. Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security.

[17]. Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799e2816. http://dx.doi.org/10.1016/ j.chb.2008.04.005

[18]. Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. Journal of information systems education, 23(4), 407-416.

[19]. Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. Journal of Broadcasting & Electronic Media, 49(1), 86-110.