Computer Security Behavior and Awareness: An Empirical Study

Nahel A O Abdallah, Odeh Abed Abdullah
Department of Information Systems, International Islamic University, Malaysia
Nahel 84@hotmail.com
Fundamentals of Religion Department, An-Najah National University, Palestine
Odeh74a@najah.edu

Abstract— The purpose of this study is to investigate the student's behavior towards information security and test critical factors that are affecting its awareness. The study was carried out among the undergraduate students of An-Najah National University, Palestine. Previous studies have shown that end-users present the weakest link in the security chain. The attacks on computer systems are continuously becoming serious problems which raise the interest among researchers. In achieving the goal of this study, surveys of 80 university students' data were collected and analyzed using SPSS to examine the theoretical model. It is hoped that the outcome of this study will contribute in developing a proper understanding of the factors influencing the behavior of university students towards information security behavior. Additionally, it is anticipated that the findings of this study to lead to more awareness programs that can be used to promote privacy and security protection behaviors of information security.

Keywords— Attitude, Information Security, Information Security Behavior, Perceived, Importance, Self-Efficacywords.

I. INTRODUCTION

Recent studies that show the advancement in technology, particularly in the field of IT have come with new scientific benefit to human beings. This is because, more than ever, people now rely solely on computers for everyday tasks, such as in their personal, educational and business purposes. Contemporarily, the use of computers by individuals of different backgrounds as proven by [1], has become a regular feature of life, in which educational sector has benefited immensely from the deployment of the computer due to its use in achieving educational goals. The reason is that, with the use of a computer, teaching and learning processes have been eminently transformed, thereby making education more attainable, unconstrained, interactive, and compelling as compared to conventional ways in education. However, the safekeeping of information has been very strenuous because of the rapid increase in modern technology as indicated by [2]. Studies have shown that among the most computer literate members of society are the university students. Based on this, it might be assumed that they should also be the most aware of the threats in using computers, particularly when dealing with on-line systems. Due to these threats issues that are happening worldwide, computer ethics and security awareness have recently raised a lot of interest among the researchers in the field of information technology [3].

The major aim of information security is to protect and prevent theft of data and information that has high value to people and organizations. As stated by [4], information security is associated with any process, task or activity that can safeguard the integrity, confidentiality, and availability of information from theft. In recent times, the security of computers has become an extremely serious issue because of the huge number of attacks on information that is occurring gradually as observed by the increasing number of security breach cases. For example, the spread of computer viruses, and hackers' invasion of proprietary network sites across the globe is enormous [5]. Statistics have shown that the huge population of more than one billion people connected to the internet worldwide, has contributed to a revolutionary impact on how they learn, interact, and communicate, making the theft of information to be more viable to risk [6].

In view of the foregoing issues mentioned above, numerous sophisticated security methods have been developed, but there has not been much improvement because information security continues to decline [7]. According to [8], no matter how well designed a security method is to protect computer information, its implementation and uses rely solely on individuals. This is in line with the study of [9] which mentioned that the success of such a security method depends on the effective behavior of individuals using it. This is because studies have proven that the human factor to be the weakest element in the security chain [10]. As identified in previous studies, academic purposes are not the only reason why students always use the internet, mainly because they also use it for personal purposes such as keeping in constant contact with

their acquaintances through e-mail, chatting, and blogs. At the same time, to date, the internet also contains numerous other websites that are operated by individuals, businesses, advocacy groups, and others that may offer incorrect or biased information [11]. Hence, based on the issues discussed above, the purpose of this research is to investigate the knowledge among university students on information security behavior and examine factors influencing their behaviors towards information security by using An-Najah University students as a case study.

II. LITERATURE REVIEW

As defined by [12], information security means "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability". However, it is also important to note that technically, information security aims at protecting the availability, accuracy, authenticity, confidentiality, integrity, utility and possession of any information [13]. To date, there are different requirements associated with information security issues. Among them are the three requirements identified as CIA (Confidentiality, Integrity, Availability), which are commonly accepted as important, regardless of the tradition of information security from which they originate [14]. However, due to the nature of the concepts, they are largely recognized only among the professional designers of information security solutions, but of less relevance to the most home users. Also, as stated by [15], the management of information security can be carried out through three separate mechanisms which are; people, policy, and technology. More so, as claimed by [8], the presence of information security in the academic setting makes it require not only technical solutions but also effective behavioral user solutions. This is because the end users are indeed the key component or factor of the computer system.

It is a known fact that computer system is important to end user; therefore, users' behavior becomes critical to information security. Based on this, security culture needs to exist among users. This is because the end user's action plays a significant role to achieve computer environment security [16]. As such, the users must comprehend how their responsibility in making good decisions on their part would lead to better security implications. Taking for example, in order to provide good background service devoid of any security risk, the users must keep their virus files and software up to date, as well as to treat email attachments with caution [17]. The reason is that; good information security practices of the users play an integral part in preventing bad computer incidents or information bridged. Apart from that, it is very important to know that single negligence from the user can cripple a strong computer security program.

Therefore, there must be an essential security practice, awareness consciousness among students using any computer system [18]. In addition, [19] explained that the criterion of protective behavior in online safety domain is updating the operating system, browser patches, virus protection, deleting cookies, and changing passwords. As identified in previous studies, there are multiple security mechanisms that still need to be engaged and updated, because of the common protections in securing computer operations (antivirus software, operating system patches, firewalls, password-based access systems as well as backup of important data).

III. THEORETICAL FRAMEWORK AND METHODOLOGY

Theories concerning individual behavior such as Social Cognitive theory [20], the Theory of Reasoned Action [21] and the Theory of Planned Behavior [22] are used to provide a foundation of the theoretical framework used in the study. Previous literature in the context of information security including important factors influencing information security behavior such as subjective norms, information security self-efficacy, perceived usefulness, and computer and internet experience are considered the main factors influencing students' information security behavior. The rationale for this selection is that these factors have shown to have significant effects on student awareness of information security Behavior in the existing literature.

To achieve the research objectives, the study applied a quantitative research method in form of the questionnaire as the data collection strategy. This would allow the researcher to provide a quantitative or numeric description of trends, attitudes, or opinions of a population by studying a sample of that population [23]. Based on the research model (Fig. 1), the interrelated set of constructs or variables are formed into hypotheses guiding the research by specifying relations among variables.

Attitude towards the behavior is defined as a person's general feeling of favorableness or unavoidableness for that behavior. Generally, the more favorable a person's attitude is towards behavior, the more likely it is that the person will want to engage in the behavior. Attitudes develop reasonably from the beliefs people hold about the object of the attitude. In the case of attitudes towards behavior, each belief links the behavior to a certain outcome, or to some other attribute. It is determined

through an assessment of one's beliefs regarding consequences arising from behavior and an evaluation of the desirability of these consequences. From information security point of view, it refers to the student's disposition responding positively or negatively towards information security. The hypothesis for this construct is:

- *H1: "Attitude towards information security has a positive relationship with information security behavior".*

At the same time, subjective norms concern with the extent to which other important people to a respondent approve or disapprove of the behavior. subjective norm can be decomposed into societal norm and social influence. According to Bandura's Social theory [24], an individual's behavior is determined by environmental influences such as social pressures. Additionally, [25] stated that external social factors such as subjective norms could influence security behavior. If social expectations are that people should engage in the behavior, then the individual should be more likely to do so. In the context of information security, this relates to a person being influenced based on their assumptions of what others believe with respect to how they should behave. Thus, it is hypothesized:

- *H2: "Subjective norm has a positive relationship with information security behavior".*

Perceived importance has been discussed in various studies as one of the factors driving individual. the usefulness of the object or activity has a positive relationship with individual motivation. An empirical study done by [26] found that perceived usefulness has significantly impacted both ethical judgment and behavioral intention. Therefore, the students who have high perceived importance of information security will have more motivation to be proactive in their information security behavior. Hence, the hypothesis is formulated:

- *H3: "Perceived Usefulness has a positive relationship with information security behavior".*

The term self-efficacy is derived from the self-efficacy construct of Bandura's [20] social learning theory. According to [27], computer self-efficacy refers to a judgment of the individual's capability to perform a task. Self-efficacy beliefs perform as an important set of proximal determinants of human motivation and action. They operate on personal behavior through motivational, cognitive, and affective intervening processes. Self-efficacy in information security is developed through the ongoing acquisition of knowledge related to information security that student receives. Literature shows that there is a positive relationship between self-efficacy and Behavior. students are more likely to value information security when they have a high level of self-efficacy in the information security domain. Therefore, the following hypothesis is proposed:

- *H4: "Self-efficacy has a positive relationship with information security behavior".*
-

Similarly, the literature shows that the internet and computer experience is another important factor affect information security behavior. As computer and Internet use become increasingly widespread, larger percentages of the population will enjoy the potential benefits and be exposed to the associated risks. [13] indicated that security-related behavior is positively and significantly correlated with the users' computer experience. [28] stated that students who know more about Internet security techniques are likely to be more aware of Internet security threats. Accordingly, the following hypothesis is proposed:

- *H5: "Year of computer and Internet experience has a significant relationship with information security behavior".*

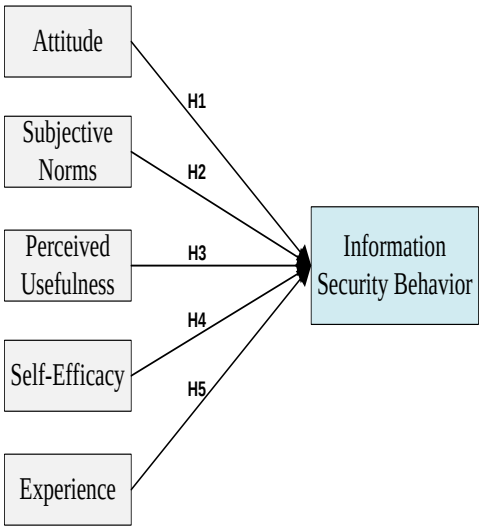

Fig 1: Research Model

The population for this study consisted of both undergraduate and postgraduate students from An-Najau National University in Palestine. Some information security practices like updating antivirus software and security patches for the operating system can be performed if an individual possesses a personal computer (PC) or laptop. The study involved all faculties within the main campus. Thus, the sample chosen in this research is students who

own a PC or laptop to quantify and assess safe computing behavior that they either protect or expose to information security attacks. The selection of participant was done through a convenience sampling approach as participants are willing and available for the study. Several rules of thumb for the minimum sample size have been proposed. A widely-accepted ratio of sample size to estimated parameters is N: p = 5:1 [29]. A ratio of five responses per parameter is required to obtain a trustworthy estimation. With a total of 20 elements, the effective sample size required to test the trustworthiness of the model would be at least 100. The survey questionnaire was used as the primary instrument in this study. the questionnaire was divided into three main sections including personal information, computer and Internet experience, as well as factors influencing information security behavior respectively. Additionally, the questions in this section were evaluated by using rating scale known as a Likert scale to assess respondent's attitudes. The respondents must answer to a seven-point Likert scale (1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 = neutral, 5= somewhat agree, 6 = agree, 7 = strongly agree). The researcher used a seven-point Likert scale to allow the respondents having more choices in their responses as well as to provide a better illustration to understand respondents' feelings or attitudes about items used in the questionnaire. Out of 200 distributed survey, only 180 responses received, out of which 4 were not included in the final data analysis because of incomplete and invalid responses. In determining whether completed questionnaires were usable or not, the completeness factor was considered. Returned questionnaires that were found to be incomplete were excluded. Responses from all respondents were free from the non-response bias and hence it can be safely assumed that those who did not respond would have a similar profile as those who did. After data screening, the final rate for this quantitative survey-based research study remained 88% which is considered a very good response rate. Then, SPSS software statistics package will be adopted to scientifically examine all data obtained from the study sample and to produce statistical data and comprehensive analyses of the questionnaire findings.

IV. RESULTS AND DISCUSSION

Reliability test is conducted to control the biases or sources of error which may occur in the measurement instruments of the study. Reliability analysis is concerned with the internal consistency and stability of a measurement instrument [30]. Based on [31], reliability analysis answers the question: "Do measures show stability across the units of observation? That is, could measurement error be so high as to discredit the finding?". To this end, Cronbach's alpha value was adopted. Reliability is usually evaluated by Cronbach's alpha [32]. Cronbach's alpha is a measure that provides a reliability coefficient to indicate the internal consistency of the instrument. Cronbach's alpha ranges from 0 (completely unreliable) to 1 (perfectly reliable) [33]. The closer Cronbach's Alpha to 1.00, the higher the reliability of the measure is. In this way of analysis, items are considered highly reliable once the overall Cronbach's alpha coefficient of all constructs is greater than 0.7. If alpha is less than this value, it indicates that the items are unlikely to be reliably measuring the same thing. Table 1 depicts Cronbach's alpha for measures used in the instrument. Most measures recorded Cronbach's alpha value greater than 0.75, suggesting that the measures are highly reliable. Therefore, there was no need to change and refine the questionnaire for increasing the alpha coefficients.

Table 1. Reliability Tests

Factor	No Items	Cronbach's alpha
Attitude	4	0.82
Subjective Norm	3	0.85
Self-efficacy	4	0.75
Perceived Usefulness	4	0.81
Information Security Behavior	5	0.80

Data about users' computer and internet experiences and respondents' characteristics collected from the sample through questionnaires. Table 2 shows the demographic profile of respondents. The profile of the respondents describes the gap difference between male and female. Out of 176 respondents, results show that Most of the respondents are female with 56.1%, while men percentage is 43.18%. Furthermore, the highest percentage of respondents (50%) have more than 6 years of computer and internet experience, followed by those who have experience between 1 to 4 years (26.7%), then between 4 to 6 years (22.1%), and less than 1 year (1.1%) respectively.

Table 2. Respondent's Experience and Demographic Profile

Item	Category	Frequency (N)	Percentage (%)
Gender	Female	100	56.81
	Male	67	43.18
Years of Experience	< 1	2	1.1
	1-4	47	26.7
	4-6	39	22.1
	>6	88	50

Similarly, correlation analysis and ANOVA are performed to find out the relationships between dependent and independent variables whether the direction of their association is positive, negative or zero. The Pearson correlation coefficients are computed among independent and dependent variables. The independent variables consist of attitude (AT), subjective norm (SN), information security self-efficacy (SE), and Perceived Usefulness of information security (PU) whereas the dependent variable is information security behavior (ISB). "The bivariate correlation analysis is conducted by calculating the Pearson correlation coefficients among variables engaged in the research. Table 3 provides the summary of the Pearson correlation matrix between variables of constructs. The Pearson *r* value shows the strength in the relationship accompanied by information about the significance of the relationship at 0.01 or 0.05 significance level (2-tailed).

Table 3. Correlation Between Independent and Dependent Variables

Variable	AT	SN	SE	PU	ISB
AT	--				
SN	0.01	--			
SE	0.33**	0.01	--		
PU	0.41**	0.25**	0.10	--	
ISB	0.34**	0.27**	0.43**	0.05	--

**Correlation is significant at the 0.01 level (2-tailed)

The result indicates that several factors are positively correlated with information security behavior. These can be observed between attitude and information security behavior (r = 0.38, $p < 0.01$), self-efficacy and information security behavior (r = 0.40, $p < 0.01$). There is also a significant relationship between subjective norm and information security behavior. (r = 0.28, $p < 0.01$). Therefore, the hypothesis (subjective norm has a positive relationship with information security behavior) is Supported. This correlation is significant at the 0.01 alpha level (2-tailed). Therefore, the findings of the study also support the hypothesis (attitude towards information security has a positive relationship with information security behavior) and the hypothesis (information security self-efficacy has a positive relationship with information security behavior). These can imply that students who have strong motivation to implement information security behavior are influenced by positive attitude and high level of self-efficacy in the information security domain. However, the Pearson product-moment correlation test did not reveal a significant correlation between perceived information security usefulness and information security behavior, (r = 0.05, $p > 0.05$). Thus, the result does not support hypothesis 3 (perceived usefulness has a positive relationship with information security behavior). This is, in turn, to be contradicted with the study by Hussein et al., [13]. On the other hand, the analysis of variance (ANOVA) is conducted to evaluate the relationship between the differences in computer and Internet experience and information security behavior (Table 4). The result shows that the relationship is statistically significant, F (2,157) = 4.26, $p < 0.05$. Thus, the last hypothesis (year of experience has a significant relationship with information security behavior) is supported.

Table 4. Analysis of Variance between Experience and Information Security Behavior

Variable	df	Mean Square	F	η2
Years of Experience	2	2.88	4.33*	0.05

Note. $R2$ = 0.05, Adjusted $R2$= 0.04, *p < 0.05

Although the effect size between the year of computer and Internet experience and information security behavior is relatively small (η2= 0.05), it indicates that the different year of computer and Internet experience in overall information security behavior depends on the safety performance (positive or negative). Information security self-efficacy makes the strongest contribution to the information security behavior followed by attitude. Fig. 2 explained the research model based on the R^2 value which is representative of the amount of variance for the dependent variable (information security behavior). The larger R^2 indicates the better predictive power of the model.

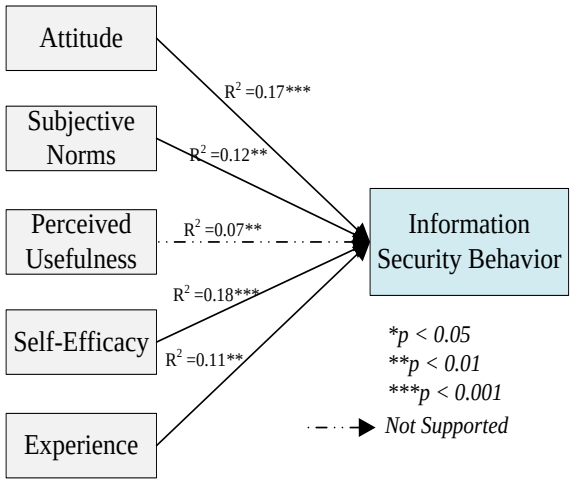

Fig2. The Research Model with R^2 Value

The study found that students have an optimistic approach towards information security practices. Role of

social influence from other believes may pay to persuade students to comply security behavior. They are inclined to believe in their own capabilities to execute the behavior. The research findings suggest that students, who have high confidence of self-efficacy towards information security, are more likely to practice information security such as updating antivirus software and protecting personal information from security breaches. Students tend to value information security and privacy when they have a high level of self-efficacy in the information security domain.

Furthermore, the study measured computer and Internet experiences in term of the year of experience. Such assortments of attributes seem to be influenced by student's behavior towards information security. Students who have many years of computer and Internet experiences are likely to take precaution less on security domain. However, the present study found out that students who spend more time using a computer and the Internet on daily routine work either for academic purposes or personal purposes can practice more information security. This implied that students may feel fear to lose their personal information as well as important data if their computers are corrupted by security attacks. "In view of the above discussions, it is apparent that the likelihood of students to demonstrate and activate security protection behavior, such as updating antivirus on a regular basis, paying attention to antivirus database updates or operating system updates when surfing the internet, using strong password for computers as well as e-mail account through voice, not sharing password with other people to protect their private information are among the important steps in combating the breach of security information as identified in this study.

V. CONCLUSIONS

Student behavioral information security perspective has been examined and identified in this study, and the key critical factors which are significant to the student behaviors towards information security are examined. Based on the result of this study, some of these factors are driven by the user's behaviour and some by the environment. It is hoped that the finding of this study will contribute in the development of a better understanding of important factors influencing the behavior of university students towards information security, and consequently leads to a more organized information security awareness programs to promote privacy and security protection behaviors. The study makes important contributions to the emerging body of knowledge on the behavioral and educational settings pertaining to information security issue. Initially, the study offers a theoretical explanation the university student's behavior towards information security. Furthermore, the research has shown that the important factors influenced on the individual can help to motivate precaution-taking behavior in information security issues. However, there are limitations to this research some of which include the study merely focuses on the factors that lead to the influence of information security Behavior among university students and it is limited to the common security practices such as antivirus software update, operating system patch, backup, and password. Thus, future study should focus on individual practices in detail, as well as other recommended security practices.

REFERENCES

[1] O. Oyewole, "Awareness and Perception of Computer Ethics by Undergraduates of a Nigerian University," *Journal of Information Science Theory and Practice*, 2017.

[2] R. L. Verecio, "Computer Ethics Awareness: Implication to Responsible Computing," *International Journal of Education and Research*, vol. 4, pp. 195-204, 2016.

[3] E. Sargolzaei and M. Nikbakht, "The Ethical and Social Issues of Information Technology: A Case Study," *International Journal of Advanced Computer Science and Applications*, vol. 8, pp. 138-146, 2017.

[4] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*: Syngress, 2014.

[5] A. R. Ahlan and M. Lubis, "Information security awareness in university: Maintaining learnability, performance and adaptability through roles of responsibility," in *Information Assurance and Security (IAS), 2011 7th International Conference on*, 2011, pp. 246-250.

[6] M. Ciampa, *Security awareness: Applying practical security in your world*: Cengage Learning, 2013.

[7] O. L. Abolarinwa, "Computer Ethics And Security Awareness Behaviour Of Tertiary Institution Students In South-Western, Nigeria," *Computer*, vol. 5, 2015.

[8] K. Šolić, K. Nenadić, and D. Galić, "Empirical study on the correlation between user awareness and information security," *International journal of electrical and computer engineering systems*, vol. 3, pp. 47-51, 2012.

[9] B.-Y. Ng, A. Kankanhalli, and Y. C. Xu, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, pp. 815-825, 2009.

[10] I. Okere, J. Van Niekerk, and M. Carroll, "Assessing information security culture: A critical analysis of current approaches," in *Information Security for South Africa (ISSA), 2012*, 2012, pp. 1-8.

[11] M. J. Metzger, A. J. Flanagin, and L. Zwarun, "College student Web use, perceptions of information credibility, and verification behavior," *Computers & Education*, vol. 41, pp. 271-290, 2003.

[12] R. C. Schaeffer, "CNSS Instruction no 4009: National Information Assurance (IA) Glossary," *Maryland: Committee on National Security Systems*, 2010.

[13] R. Hussein, F. Lambensa, and R. B. Anom, "Information security behaviour: a descriptive analysis on a Malaysian public university," 2011.

[14] W. Conklin, *Computer security behaviors of home PC users: A diffusion of innovation approach*: The University of Texas at San Antonio, 2006.

[15] M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations," 2018.

[16] N. N. A. Molok, A. M. Ali, S. Talib, and M. Mahmud, "Information security awareness through the use of social media," in *Information and Communication Technology for The Muslim*

World (ICT4M), 2014 The 5th International Conference on, 2014, pp. 1-6.

[17] F. A. Aloul, "The need for effective information security awareness," *Journal of Advances in Information Technology*, vol. 3, pp. 176-183, 2012.

[18] C. P. Garrison and O. G. Posey, "Computer Security Awareness of Accounting Students," 2006.

[19] R. Yilmaz, F. G. Karaoglan Yilmaz, H. T. Özturk, and T. Karademir, "Examining Secondary School Students' Safe Computer and Internet Usage Awareness: An Example from Bartin Province= Lise Ögrencilerinin Güvenli Bilgisayar ve Internet Kullanim Farkindaliklarinin Incelenmesi: Bartin Ili Örnegi," *Online Submission*, vol. 7, pp. 83-114, 2017.

[20] A. Bandura, "Social foundations of thought and action," *Englewood Cliffs, NJ*, vol. 1986, 1986.

[21] M. Fishbein and I. Ajzen, *Belief, attitude, intention and behavior: An introduction to theory and research*, 1975.

[22] I. Ajzen, "From intentions to actions: A theory of planned behavior," in *Action control*, ed: Springer, 1985, pp. 11-39.

[23] J. W. Creswell and J. D. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications, 2017.

[24] A. Bandura, "1986. Social foundations of thought and action. A social cognitive theory," *Englewood Cliff*.

[25] S. M. Galvez and I. R. Guzman, "Identifying factors that influence corporate information security behavior," *AMCIS 2009 Proceedings*, p. 765, 2009.

[26] T. P. Cronan, L. N. Leonard, and J. Kreie, "An empirical validation of perceived importance and behavior intention in IT ethics," *Journal of Business Ethics*, vol. 56, pp. 231-238, 2005.

[27] D. R. Compeau and C. A. Higgins, "Computer self-efficacy: Development of a measure and initial test," *MIS quarterly*, pp. 189-211, 1995.

[28] G. Y. Jaw and J. Y. Chen, "Asian new generation's perceptions regarding
network fraud. Second International Conference on Innovative Computing,
Informatio and Control," presented at the Second International Conference on Innovative Computing,
Informatio and Control
Kumamoto, Japan, 2007.

[29] R. B. Kline, *Principles and practice of structural equation modeling*: Guilford publications, 2015.

[30] N. Blaikie, *Analyzing quantitative data: From description to explanation*: Sage, 2003.

[31] D. W. Straub, "Validating instruments in MIS research," *MIS quarterly*, pp. 147-169, 1989.

[32] H. M. Selim, "An empirical investigation of student acceptance of course websites," *Computers & Education*, vol. 40, pp. 343-360, 2003.

[33] B. R. Lewis, G. F. Templeton, and T. A. Byrd, "A methodology for construct development in MIS research," *European Journal of Information Systems*, vol. 14, pp. 388-400, 2005.