International Academic Institute for Science and Technology

International Academic Journal of Social Sciences Vol. 4, No. 1, 2017, pp. 120-130.

ISSN 2454-3918

International Academic Journal of Social Sciences

www.iaiest.com

Effect of Perceived Security and Perceived Privacy towards Trust and the Influence on Internet Banking Usage among Malaysians

Normalini Md Kassim[1]

[1]School of Management, Universiti Sains Malaysia, Minden Penang, Malaysia

Abstract

Internet banking security is a critical issue over the world. But the traditional protection mechnisms are not sufficient to secure the online banking systems that hold information about clients, and banks. The objective of the present study was to identify the impact of perceived security and privacy factors on customer trust and its influence on intention to continue using Internet banking in Malaysia. The participants for this study were individual Internet banking users in Peninsular Malaysia. Data was collected through self-administered questionnaires distributed using the drop-off and pick-up (DOPU) technique to bank branch managers who then passed the questionnaires to their customers. A total of 413 respondents completed the questionnaires. The SPSS statistical analysis software package and Partial Least Squares statistical method were used for data analysis and hypothesis testing. The results show that perceived security significantly influences customer trust and consequently intention to continue using Internet banking. Moreover, trust plays a critical role in influencing intention to continue using Internet banking in Malaysia while perceived privacy does not. An understanding of the factors identified in this study will enable Internet banking providers to effectively and efficiently enhance the security of services and thereby promote continued usage of Internet banking among customers. The findings of this study are thus expected to be of great use to Internet banking providers as improvements in Internet banking security will increase business in the long run.

Keywords: Internet, Banking, Security, Privacy, Trust

INTRODUCTION

Internet banking has provision networks that replaces and replicated various activities currently executing by the bank. According to Zahoor et al. (2017) the usage of internet banking significantly affects the customers trust due to unavailablility of cyber security. The outcome from their research indicates the essential challenges faced by the banking industry in Pakistan are cyber threats due to internet connectivity such as transactions security, privacy of customers' accounts-threat and banking system security. Internet banking security and privacy concerns are prevalent owing to threats arising from internet networks and electronic transactions. Authentication failures in internet systems lead to

unauthorized account access and retrieval of personal financial information, creating anxiousness among customers using Internet banking services. Online banking service providers, recognizing customer concerns, are beginning to utilize a number of technologies that have been developed to ensure the security and privacy of electronic transactions. However, the safety of these transactions remain a concern for Internet banking customers (Sathye, 1999).

A study conducted in Australia found that the key impediments to customer adoption of Internet banking were security concerns and the lack of familiarity with Internet banking (Sathye, 1999). Many similar studies conducted in Malaysia and other countries have examined trends in adoption of Internet banking and causes of delayed growth. Security and personal preference factors are among the reasons found to hinder the growth and adoption of Internet banking in Malaysia (Suganthi, Balachandher, & Balachandran, 2001).

Analysing current Internet banking security trends and issues creates great trepidation; Internet banking crimes keep increasing by the day. Considering the importance of security and privacy in online banking transactions, the key security and privacy factors influencing customer intention to continue using Internet banking were investigated in this study. Therefore, the findings from this research could provide important clues on the extent of enhancements that should be done to improve the level of security and privacy in Internet banking. The ourcome of this research may add to the literature on understanding in-depth the characteristics of the perceived security such as Authentication, Non-repudiation, Data Integrity and Confidentiality. Besides the common authentication security, we might have the solution by integrating multi- factor authentication such as on biometrics technologies implementation.

LITERATURE REVIEW

Existing literature has found various factors that influence adoption of Internet banking technology. Banks need to identify relevant issues that shape adoption patterns to make important enhancements that meet customer needs, create demand and facilitate the expansion of Internet banking. In this study, literature on perceived security, perceived privacy, trust and intention to continue using Internet banking have been examined and found to be important factors that are relevant to Internet banking. Thus, these form the constructs in the research framework and are defined below.

Perceived Security

The need for security has already been recognized by electronic commerce and banking providers. Security concerns in the context of Internet banking include threats made through networks involving data transactions or unauthorized access to accounts due to authentication failures by means of false or defective authentication. Perceived security, then, is the "customers' perception of the degree of protection against these threats" (Yousafzai, Pallister, & Foxall, 2003). Customers are afraid that their personal financial information will become available to others via the internet and used for fraudulent purposes. According to Yousafzai et al. (2009), customers' subjective views regarding the security of internet banking transactions can be measured based on their perceptions of timely, accurate, and safe data transmission.

Perceived Privacy

Consumer privacy, as termed by Goodwin (1991), is "the consumer's ability to control (a) the presence of other people in the environment during a market transaction or consumption behaviour, and (b) dissemination of information related to or provided during such transactions or behaviours to those who were not present". Perceived privacy on the other hand, is defined by Yousafzai et al. (2003) as the

"customer's perception regarding their ability to monitor and control information about themselves". Trust stemming from perceived privacy can most likely be reached by letting the balance of power shift towards greater collaborative interaction between online businesses and their customers (Hoffman and Novak, 1997, as cited in Hoffman, Novak and Peralta, 1999). The balancing of power to obtain trust involves, among other things, the recognition of a consumer's right to data ownership during online transactions. Hoffman, Novak and Peralta (1999) found that trust issues derive from the perceived lack of control over a consumer's personal information and the access others have to the information during the online navigation process. There is thus an implication that confidentiality, an important aspect of building trust, can possibly be lost in such online processes (Culnan & Armstrong, 1999).

Trust

Social psychologists define trust as an expectation about the behaviour of others in transactions and focus on the contextual factors that enhance or inhibit the development and maintenance of trust (Lewieki & Bunker, 1995). According to Mayer, Davis, and Schoorman (1995) as well as Rousseau, Sitkin, Burt, and Camerer (1998), customer trust in electronic banking is defined as, "a psychological state which leads to the willingness of a customer to perform banking transactions on the Internet based on the expectation that the bank will fulfil its obligations, irrespective of the customer's ability to monitor or control the bank's actions".

Intention to Continue Using

Behavioural intention measures a person's relative strength of intention to display a specific behaviour. It is likely that a person will adopt a specific behaviour if he or she intends to do so. This implies that behavioural intention (BI) to continue using Internet banking is expected to have a positive influence on users' interactions with online banking systems.

METHODOLOGY

Information security, which is not only a technical problem, but also related to human factors, is a great concern among internet users. Thus, the problem of information security is becoming an increasingly essential issue. For common internet users, information security may mean "being able to work with computers without being attacked by viruses", "being able to conduct on-line business without worrying that the credit card numbers will be stolen" or "being able to read e-mails without receiving spam". The number of threats to information security is almost uncountable and is on the rise (Ding-Long, Pei-Luen, & Salvendy, 2007). The main issues in Malaysia related to Internet banking are weak security and lack of trust in Internet banking applications. Therefore, this study will investigate the effect of perceived privacy and security factors on trust and its influence on user intention to continue using Internet banking (refer to Fig.1).

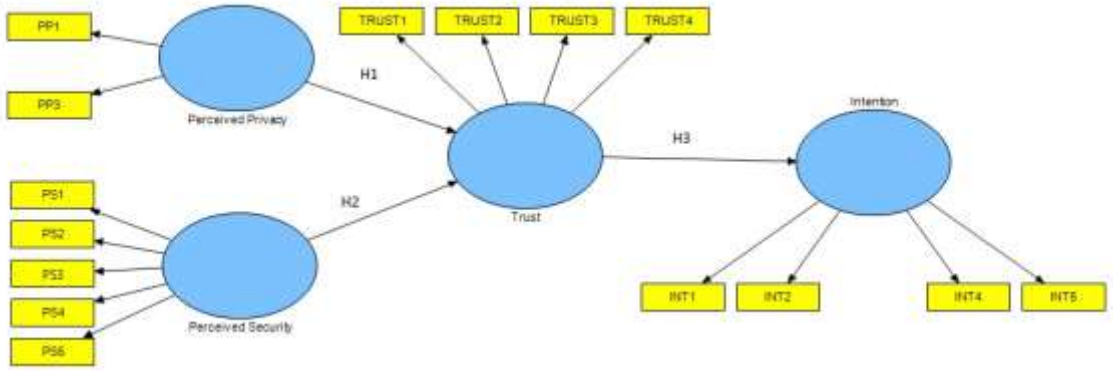


Fig. 1 Research Framework

Results

To analyse the data collected, the partial least squares (PLS) method was used. The Smart PLS 3.0 (Ringle, et al., 2014) software and two–step approach suggested by Anderson and Gerbing (1988) were adopted for data analysis. Following the suggestion of Chin (1998), the bootstrapping method (500 resamples) was also used to determine the significance levels for loadings, weights and path coefficients. All measures were adapted from published literature (see Table 1).

Table 1. Questionnaire items used in this study

Constructs	Questionnaire items
Perceived Privacy	Internet hackers (criminals) might take control of my checking account if I used Internet Banking What are the chances that using Internet Banking will cause you to lose control over the privacy of your payment information? My signing up for and using an Internet Banking lead to a loss of privacy for me because my personal information would be used without my knowledge.
Perceived Security	While using Internet banking, I believe that the security system will confirm my identity before ***disclosing*** account information. While using Internet banking, I believe that the security system will confirm my identity before ***processing*** transactions. While using Internet banking, I believe that the security system provides a secure environment in which to bank While using Internet banking, I believe that the security system does not allow unauthorized access to the account. While using Internet banking, I believe that the security system stops any unauthorized changes to a transaction.
Trust	My Internet banking site is trustworthy My Internet banking site keeps its promises and commitments I trust my Internet banking site I trust my bank

Intention to Continue Using	I intend to continue using Internet banking services rather than discontinue its use.
	My intentions are to continue using Internet banking services than use any alternative means (traditional banking).
	If I could, I would like to discontinue my use of Internet banking services.
	I intend to continue using Internet banking services whenever I need it
	I intend to continue using Internet banking service feature since it is good

Demographic Profile of the Sample

Table 2 shows the demographic profile of the respondents. Eight demographic characteristics were specifically studied: gender, age, race, highest academic qualification, occupation, total years of working experience, total years of Internet usage and total years of Internet banking. The gender of respondents was almost equal, with 58.6 per cent female and 41.4 per cent male. The majority of respondents were young and middle aged adults, with almost 78.5 per cent in the range of 20 to 39 years old. As expected, the respondents were highly educated and the majority of them had academic qualifications, namely, certificate or diplomas (16 per cent), degrees (43.6 per cent) and postgraduate qualifications (22.5 per cent). The majority of respondents were of Malay or Bumiputra ethnicity, with 72.2 per cent of respondents from this category. Respondents were mostly professionals (52.3 per cent) while 18.9 per cent of respondents were under the category of 'others' as they held executive level positions (for example: marketing executive, auditor, bank executive, finance officer and HR officer). Almost all respondents had work experience and most of them had worked for at least 1 to 20 years (91.40 per cent). The fact that 98.40 per cent of respondents had used the Internet for a period of 1 to 20 years suggests that this could be due to the fact that most of them were working with access to the Internet. However, only 73.2 percent of respondents had used Internet banking for more than three years.

Table 2. Profile of Internet Banking Respondents

Demographics	Categories	Frequency	%
Gender	Male	171	41.4
	Female	242	58.6
Age	< 20	1	0.2
	20-29	132	32.0
	30-39	192	46.5
	40-49	64	15.5
	>50	24	5.8
Race	Malay/ Bumiputra	298	72.2
	Chinese	71	17.2
	Indian	35	8.5
	Others	9	2.2
Highest Academic Qualification	SPM or equivalent	51	12.3
	STPM or equivalent	23	5.6
	Certificate/Diploma	66	16.0
	Degree	180	43.6
	Post-Graduate	93	22.5

Occupation	Professional	216	52.3
	Housewife/Husband/Self-employed	11	2.7
	Clerical Staff	65	15.7
	Technical Staff	42	10.2
	Others (Please specify)	78	18.9
	Missing	1	0.2
Total years of working experience	<1 year	1	0.2
	1-10 years	242	58.6
	11-20 years	135	32.8
	21-30 years	23	5.5
	>30 years	12	2.8
Total years of Internet usage	1-10 years	273	66.1
	11-20 years	133	32.3
	21-28 years	7	1.60
Total years of Internet banking	<3 years	111	26.8
	3-6 years	212	51.3
	7-11 years	90	21.9

Assessment of the Measurement Model

Convergent validity is the degree to which the items that are indicators of a specific construct converge or share a high proportion of variance in common (Hair et al, 2010). According to Hair et al.
(2010), factor loadings and average variance extracted (AVE) values of more than 0.5 and composite reliability (CR) values of 0.7 and above are deemed to be acceptable. As can be seen from Table 3, all loadings and AVE values are above 0.5 while CR values are more than 0.7. Therefore, we can conclude that convergent validity has been established. Next, the discriminant validity, which is the extent to which a construct is truly distinct from other constructs (Hair et al., 2010), was established. This was established by the low correlations found between all the measures of interest and the measures of other constructs. To ascertain discriminant validity, the square root of the AVE is compared against the correlations of other constructs. When the AVE extracted is greater than its correlations with all other constructs, then discriminant validity has been established (Fornell and Larcker, 1981) (refer Table 4). Reliability, which is the degree of consistency between multiple measurements of a variable, is measured to ensure that the individual indicators of the scale are measuring the same construct, and thus are highly intercorrelated (Nunnally, 1978). Reliability can be assessed using CR values. Based on Table 3, the CR values were in the range of 0.837 to 0.964 and thus exceeded the cut-off value of 0.7 suggested by Hair et al. (2010). As such, based on the values of CR, it can be concluded that the measurement model is reliable.

Table 3. Results of the measurement model

Construct	Item	Loadings	AVE[a]	CR[b]
Perceived Privacy	PP1	0.681	0.727	0.837
	PP3	0.995		
Perceived Security	PS1	0.881	0.837	0.962
	PS2	0.923		
	PS3	0.938		
	PS4	0.927		
	PS5	0.904		
Trust	TRUST1	0.921	0.869	0.964
	TRUST2	0.943		
	TRUST3	0.950		
	TRUST4	0.915		
Intention to continue using IB	INT1	0.944	0.860	0.961
	INT2	0.897		
	INT4	0.942		
	INT5	0.925		

Notes: PP2 and INT3 were deleted due to low loadings

[a] Average variance extracted (AVE) = (summation of the square of the factor loadings)/{(summation of the square of the factor loadings) + (summation of the error variances)}
[b] Composite reliability (CR) = (square of the summation of the factor loadings)/{(square of the summation of the factor loadings) + (square of the summation of the error variances)}

Table 4. Discriminant validity of constructs

	Intention	Perceived Privacy	Perceived Security	Trust
Intention	**0.927**			
Perceived Privacy	-0.005	**0.853**		
Perceived Security	0.547	-0.029	**0.915**	
Trust	0.760	-0.012	0.592	**0.932**

Notes: Diagonal elements are the square root of average variance extracted (AVE) between the constructs and their measures. Off-diagonal elements are correlations between constructs. For discriminant validity, diagonal elements should be larger than off-diagonal elements in the same row and column.

Assessment of the Structural Model

The structural model represents the relationships between constructs or latent variables that were hypothesized in the research model. The goodness of the theoretical model is established by the variance as well as the R^2 and path coefficient values which indicate how well the data supports the hypothesized model (Chin, 1998). Table 5 shows the results of the structural model from the PLS output. Perceived

Security was found to be significantly related to Trust (b = 0.593, p < 0.01) and Trust to Intention to continue using Internet banking (b = 0.760, p < 0.01), thus supporting H2 and H3 of this study. However, Perceived Privacy was not a significant predictor to Trust (b=0.005, p>0.05), H1 was not supported.Trust explained 57.8 per cent of the variance in Intention. A closer look at the findings reveals that Trust is the strongest predictor of Intention to continue using Internet banking followed by Perceived Security respectively. Apart from that, the 'blindfolding' procedure was also performed to measure the predictive relevance (Q^2) of the model fit. The Q^2 'represents a measure of how well observed values are reconstructed by the model and its parameter estimates' (Chin, 1998). Models with Q^2 values greater than zero imply that the model has predictive relevance. Table 6 shows the result of the blindfolding tests. An omission distance of 7 was utilized as Chin (1998) indicates that values between 5 and 10 are feasible (refer to Table 6). The goodness of fit (GoF) of the model was also calculated to assess the performance of the model. Table 5 shows the result of the GoF.

Table 5. Summarized results of hypotheses testing

Hypothesis	Relationship	Beta	Std Error	t-value	Decision
H1	**PP->Trust**	0.005	0.055	0.091	Not Supported
H2	**PS->Trust**	0.593	0.043	13.79***	Supported
H3	**Trust->Intention**	0.760	0.037	20.732***	Supported

Notes: ***p<0.01(2.33), **p<0.05(1.645), *p<0.1(1.28); (based on the one-tailed test)

Table 6. Blindfolding results: cv-communality and cv-redundancy

Block	Cv – Communality H^2	Cv- Redundancy F^2
Trust	0.865	0.303
Intention	0.741	0.494

DISCUSSION

The model of e-trust banking by Yousafzai et al. (2003) was used as the basis for information system (IS) acceptance in this study. The framework developed in this research incorporates the main dimensions of security to identify factors that influence intention to continue using Internet banking; namely perceived privacy, perceived security dimensions and trust. The rationale for causal relationships developed in the framework is based on combined theoretical frameworks. Mukherjee and Nath (2007) stated that the privacy and security features of websites along with shared values are key antecedents of trust, which in turn positively influence the behavioural intentions of customers. The development of trust affected the intention to conduct transactions and trust was particularly influenced by consumers' perceived security related to the handling of their personal data (Flavián and Guinalíu, 2006). Unexpectedly, this research has found that perceived privacy has an insignificant impact on customers' trust in Internet banking. An explanation of this finding might be that Internet banking customers in Malaysia have the perception that other issues such as security are more important and serious compared to privacy issues. According to Kim, Steinfield, and Lai (2008), empirical evidence shows that security protection mechanisms are more important in affecting consumers' behaviour than privacy. Another possible explanation is that the strong privacy policies which are enforced by the Internet banking providers create customer confidence in

Internet banking. The results of the descriptive analysis for customers' demographics (Table 2) clearly show that the majority of respondents were experienced Internet banking users since those with Internet banking experience of more than 3 years was 73.2% (combined total of 51.30% for 3 to 6 years of experience and 21.90% for 7 to 11 years of experience). Therefore, it may be that experienced Internet banking customers are familiar with security related technology and easily recognize features such as security certificates or encryption keys. Given that these security characteristics guarantee almost total privacy, the relative importance of privacy concerns for these users is comparatively lower. Thus, the presence of security features fosters trust in Internet banking and eases the decision to disclose personal and financial information. Therefore, perceived privacy does not significantly influence customers' trust in Internet banking. On the other hand, perceived security has been proven to have a significant positive impact on customers' trust associated with the use of Internet banking. The rational justification of this finding might be that once the perceived strength of security is high, an increased level of customers' trust in using Internet banking is then possible. In this study, it has been proven that trust has a significant positive impact on intention to continue using Internet banking. In other words, a high level of trust in Internet banking may increase the level of intention to continue using Internet banking. The rational justification of this conclusion might be that once Internet banking customers in Malaysia have confidence in the reliability of Internet banking, they might have positive feelings about conducting banking transactions online via the use of Internet banking.

CONCLUSION

This research may help to enhance and deepen understanding of the IS acceptance model as it has been applied to Internet banking and incorporated with factors that affect intention to continue using Internet banking. Rationale for causal relationships in the model have been developed based on combined theoretical frameworks, providing further insights on factors influencing adoption of Internet banking. Several important implications arise from the results of this study. This research identifies factors that impact customers' intention to continue using Internet banking in Malaysia and thus provide important and comprehensible insights for practitioners in the banking industry. The outcome of this study is crucial as it can lead to greater awareness among banking institutions in Malaysia about the importance of security and trust in Internet banking. The answers provided in this study hold the key to enhancing the level of security in Internet banking and could also help banks to devise marketing strategies that promote online banking applications in the future.

ACKNOWLEDGEMENTS

The authors acknowledge all reviewers for their comments on this manuscript and are grateful to the committee members of the Regional Conference on Science Technology & Social Sciences (RCSTSS2016) for organising a beneficial conference that has provided a good platform for research development in this field. The research reported in this article was funded by University of Science Malaysia Short Term Grant number 304/PMGT/6313098.

REFERENCES

Anderson, James C., and David W. Gerbing (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach, *Psychological Bulletin*, 103 (3), 411–423.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In Marcoulides, G. A. (Ed.), *Modern business research methods*. Mahwah, NJ: Lawrence Erlbaum Associates.

Culnan, M.J., & Armstrong, P.K. (1999)," Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," Organization Science, 10(1), 104-115.

Ding-Long, Huang, Pei-Luen, Patrick Rau, & Salvendy, Gavriel. (2007). A Survey of factors Influencing People's Perception of Information Security. *Human Computer Interaction*, 906-915.

Flavia´n, C. and Guinalı´u, M. (2006)," Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site," Industrial Management & Data Systems, 106(5), 601-620.

Fornell, C., & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. . *Journal of Marketing Research, 18*(1), 39-50.

Goodwin, C. (1991), "Privacy: Recognition of a consumer right," Journal of Public Policy Marketing, 10(1) (Spring 1991), 106-119.

Hair, J.F., Black, William C., Babin, Barry J., & Anderson, Rolph E. (2010). *Multivariate data analysis. (7th ed.)*. Pearson, Upper Saddle River.

Hoffman, D.L., & Novak, T. P. (1997)," A new marketing paradigm for electronic commerce," information Society: An International Journal, 13(1), 43-54.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999),"Building consumer trust online," Communications of the ACM, 42(4), 80-85.

Kim, D.J., Steinfield, C., & Lai, Y. (2008). Revisiting the role of web assurance seals in business-to-consumer electronic commerce. Decision Support Systems, 44(4), 1000-1015.

Lewieki, R.J., & Bunker, B. B. (1995)," Trust in relationships: a model of trust development and decline," In Bunker, B.B. (Ed): Rubin, J.Z. (Ed), (1995). Conflict, cooperation, and justice: Essays inspired by the work of Morton Deutsch. The Jossey-Bass management series and The Jossey-Bass conflict resolution series, (pp. 133-173). San Fransisco, CA, US: Jossey-Bass.

Mayer, R.C., Davis, J.H., & Schoorman, F.D. (1995)," An integrative model of organizational trust," Academy of Management Review, 20(3), 709-734.

Mukherjee, A. and Nath, P. (2007),"Role of electronic trust in online retailing: a re-examination of the commitmenttrust theory," European Journal of Marketing, 41(9/10), 1173-1202

Nunnally, J.C. (1978). *Psychometric theory*. New York, NY: McGraw-Hill.

Rousseau, D.M., Sitkin, S.B., Burt, R.S., & Camerer, C. (1998),"Not so different after all a cross-discipline view of trust," Academy of Management Review, 23(3), 393-404.

Ringle, Christian M., Wende, Sven, & Becker, Jan-Michael. (2014). Smartpls 3. Hamburg: SmartPLS. Retrieved from http://www.smartpls.com

Sathye, M. (1999)," Adoption of Internet banking by Australian consumers: an empirical investigation," International Journal of Bank Marketing, 17(7), 324-334

Suganthi, r., Balachandher, k.g. & Balachandran, S. (2001)," Internet banking patronage: an empirical investigation of Malaysia," Journal of Internet Banking and Commerce, 6(1). www.arraydev.com/commerce/JIBC/0103_01.htm

Yousafzai, S. y., Pallister, J. G., & Foxall, G.R. (2003),"A proposed model of e-trust for electronic banking," Technovation, 23(11), 847-860.

Yousafzai, S., Pallister, J., & Foxall, G. (2009),"Multi-Dimensional Role of Trust in Internet Banking Adoption," The Service Industries Journal, 29(5), 591-605.

Zahoor,H., Dayal,D., Zulfiqar, A.B., Muhammad Hammad-u-Salam, Fauzia, T., and Glub, R. (2017). E-Banking Challenges in Pakistan: An Empirical Study. Journal of Computer and Communication, 5, 1-6