PERCEIVED RISK TOWARDS CONTINUAL USAGE INTENTION OF ONLINE BANKING

M. T. Hirnissa1*, M.A. Zariyawati2 and T. Ying-Ying3

1 Kolej Universiti Poly-Tech Mara, Kuala Lumpur, Malaysia
2 3 Faculty of Economics and Management, Universiti Putra Malaysia
*Corresponding author: hirnissa@kuptm.edu.my

Abstract: This study aims to determine the perceived risk towards continual usage intention of online banking in Malaysia. The perceived risk variables are adopted from Theory of Perceived Risk to further examine the influence to continual usage intention of online banking in Malaysia which included privacy risk, financial risk, social risk, time risk, performance risk and psychological risk. This research was distributed through online questionnaire by using convenient sampling technique to collect the data. A total of 400 respondents were obtained from online banking user who are above 18 years old in Malaysia. Multiple Linear Regression analysis was used to analyze the relationship between perceived risk and continual usage intention of online banking in Malaysia. The result revealed two perceived risks (time risk and psychological risk) were found to significantly influence the continual usage intention of online banking in Malaysia.

Keywords: Online Banking, Perceived Risk, Continual Usage Intention, Malaysia

1. Introduction

Online banking defines as a banking activity is implemented by using internet as the delivery channel such as funds transfer, mortgages payment as well as billing, checking savings bank account, buying financial instruments and certificates of deposits (Singhal & Padmanabhan, 2008). Nowadays, online banking service is a significant driving force in the financial banking industry (Aliyu, Rosmain & Takala, 2014). One of the most effective banking transaction method is online banking rather than the offline banking approach (Lee, 2009). Online banking delivers efficient and prompt financial services and provide advantages for users such as ease of use, convenient and decrease transaction cost by using online banking service (Aliyu, Rosmain & Takala, 2014). According to payment statistic by Bank Negara Malaysia, a total number of 2.6 million internet banking users (which penetration to population of (9.8%) in 2005 increased to a total of 25.5 million users (79.6%) by 2017. It is worth acknowledging that Malaysia has 31 banks offering Internet banking service in June 2015, conducting more than 210 million banking transactions with a value of 2.33 billion Ringgit (Malaysia Financial Service, 2015). Online banking has carried great potential and improvement for bank to develop financial industry in Malaysia.
Rapid development of internet banking capabilities also brings a lot of risk to the internet banking user. Online banking is a common platform to perform the transaction through internet. Issue security occurred in online banking recently have influenced the customer to reconsider whether to continue using the online banking in future. The online banking have also its own security weaknesses that could easily become the target of criminal. There is no perfect security system can be protect security of your bank completely. The criminal will find its way to exploit the security loopholes in order to steal the information through unauthorized access and gain more profit via illicit activities. In the online banking, hacker will try to hack customer bank accounts through phishing, hacker attacks, malware and other unauthorized activity.

The failure in cyber security has recently became prevalent and threatened the security of online banking in Malaysia. Cyber-criminal issues will cause the perceived risks of online banking users to increase and lead users to reconsider continual usage intention of online banking. The consumer's perceived risk could influence the use of service technology (Paluch & Wünderlich, 2016). Malaysia is among the 10 countries that is most affected by online banking malware (Goh, 2014). The first ranked country is United States (23%) with over 26,000 online banking malware detections, Japan (10%) came in second, India ranked third with (9%), Brazil ranked fourth with (7%), followed by Turkey (4%), then France, Malaysia, Mexico, Vietnam and Australia with 3% respectively. Hence, the report indicate that Malaysia is not spared from the online banking malware menace and influence though internet banking (Victor Lo, South-East Asia regional consulting director at Trend Micro, 2014). This study aims to determine the perceived risk towards continual usage intention of online banking in Malaysia.

2. Literature Review

The user’ continual usage intention can be defined that user intention continue to use in the future. Previous research states that behavioral intention as strong role in shaping the actual usage and adoption of particular technology or systems (Alalwan, Dwivedi & Rana, 2017). The behavioral intention will have important positive influence on technology usage (Martins, Oliveira & Popović, 2014). The perceived risks as a negative factor influence the intention behavioral user. Perceived risk of user might decrease user belief and intention making internet transaction (Yang, Pang, Liu, Yen & Tarn, 2015). Apart from that, perceived risk can defined that online banking user could feel uncertainty and insecure when they suffer potential loss after experienced the unpleasant outcome. Diverse perceived risk come from different perspective of user. According to the Bauer (1967) perceived risk is interpreted as a combination uncertainty and crucial consequences. Then, potential loss is a risk when pursuit a desired outcome in E-service (Paluch & Wünderlich, 2016). Perceived risk could classified into six types which are financial risk, performance risk, time risk, psychological risk, social risk and privacy risk (Paluch & Wünderlich, 2016). Possible negative consequence of using online banking make user uncertainties (Yousafzai, Pallister & Foxall, 2003). Risk and uncertainty are interrelated whilst the uncertain consequences are considered as risk (Littler & Melanthiou, 2006). The perceived risk can defined as a possible loss when pursue desired result (Sanayei & Bahmani, 2012).
The perceived risk variables are adopted from Theory of Perceived Risk (TPR) to further examine the influence of continual usage intention through online banking in Malaysia which included privacy risk, financial risk, social risk, time risk, performance risk and psychological risk (Featherman & Pavlou, 2003). The constructs of perceived risk first come out from the Bauer (1960) seminal statement to investigate various aspects of consumer behavior. Five types of perceived risk extracted from the Bauer's original work which are financial, performance, physical, psychological, and social risk as found in (Jacoby & Kaplan, 1972).

Previous research by Roselius (1971) show that time loss is one of the perceived risk in (Jacoby & Kaplan, 1972). Cunningham (1967) further typifies that perceived risk as having six dimensions namely performance, financial, opportunity/time, safety, social, and psychological loss to examine the e-services adoption. According to Featherman & Pavlou (2003) safety risk is not included in the study adoption of e-service because it does not present any threat to human life. However, e-service users might consider the theft and loss of personal financial information, which makes privacy risk instead of safety risk to be included within the risk dimensions. This research adopts six perceived risks such as financial risk, performance risk, time risk, psychological risk, social risk and privacy risk to determine the relationship towards continual usage intention of online banking (Featherman & Pavlou, 2003).

3. Methodology
This study interprets data through quantitative analysis, since the purpose of this study is to examine the significant relationship of perception risk towards user’s continual usage intention of online banking. This study distributed online questionnaire throughout Malaysia, using convenient sampling technique to determine the relationship between the factors of perceived risk towards the continual usage intention of online banking. The researcher use IBM Statistical Package for the Social Sciences (SPSS) software to analyze data from the questionnaire. The data was collected from 400 online banking users in Malaysia who are above 18 years old. Several other analyses including in study such as Common Method Variance, Frequency Analysis, Reliability test, Descriptive Analysis and Normality test to measure the validity of data. To ensure in this research that there is no bias on common method variance, we used Harman’s Single Factor analysis in Exploratory Factor Analysis (EFA) to determine the percentage of variance loading on the first factor.
Figure 1: Theoretical Framework

Hypotheses Testing
Hypothesis 1: There is a significant relationship between privacy risk and continual usage intention of online banking.

Hypothesis 2: There is a significant relationship between financial risk and continual usage intention of online banking.

Hypothesis 3: There is a significant relationship between social risk and continual usage intention of online banking.

Hypothesis 4: There is a significant relationship between time risk and continual usage intention of online banking.

Hypothesis 5: There is a significant relationship between performance risk and continual usage intention of online banking.

Hypothesis 6: There is a significant relationship between psychological risk and continual usage intention of online banking.

4. Results and Discussion
The SPSS result of CMV indicates that the total variance is 15.957 and 48.356% < 50% which means that there is no bias Common Method Variance in this study. The reliability test is to examine internal consistency of the study. Cronbach’s Alpha as a tool to determine internal reliability. There are 33 items to measure the reliability of the variables. The alpha coefficient ranges between 0.6-0.7 is considered fair reliability, whereas the alpha between 0.7-0.8 is a good reliability. The Cronbach’s alpha 0.8 and above are all considered to be very reliability. The Cronbach’s Alpha result of reliability test on privacy risk (0.866), financial risk (0.882), social risk (0.871), time risk (0.867) and performance risk (0.882) and continual usage intention (0.905)
which are within the range of 0.8 and above that it will considered very good reliability. Besides that, psychological risk (0.795) considered as good reliability.

The normality test is used to measure the parametric data in the population which must be normally distributed. Data also can consider normal if the skewness is between -1 and +1. Apart from that, the value +/-2 still can be acceptable (Pallant, 2001). The skewness of variables falls between -1 and +1 level on privacy risk (Skewness = 0.566, M = 2.78, SD = 0.755), financial risk (Skewness = 0.508, M = 2.69, SD = 0.785), social risk (Skewness = 0.568, M = 2.50, SD = 0.697), time risk (Skewness = 0.659, M = 2.42, SD = 0.688), performance risk (Skewness = 0.573, M = 2.66, SD = 0.741) and psychological risk (Skewness = 0.610, M = 2.50, SD = 0.716).

According to Cohen (1988), R value (0.636) indicates continual usage intention have strong relationship with 6 independent variables. The coefficient of determination, $R^2$ = 0.404 explain that 40.40% variance in continual usage intention of online banking is explained by privacy risk, financial risk, social risk, time risk, performance risk and psychological risk. The p-value is 0.000 < 0.05 and F-value is 41.077 that the regression model fit the data. The overall multiple regressions model is significant at the 5% level of significance and the regression model is a good relationship between dependent variable to six independent variables.

Multiple regression analysis is implemented to determine significant relationship between the independent variables and dependent variable. The result revealed that there are two perceived risks which were found to be significant to influence the continual usage intention of online banking in Malaysia, there are time risk ($\beta$ = -0.195, p < 0.05) and psychological risk ($\beta$ = -0.265, p < 0.05). This study contributed to banks and online banking user to better understand, which perceived risk is more crucial to affect the continual usage intention of online banking in Malaysia. Apart from that, the findings in this paper can contribute as a guideline and reference for future researchers who intend to do their future research in similar area.

The psychological risk ($\beta$ = -0.272) has the highest coefficient, which is contributes the most among the variables to the continual usage intention of online banking among the 6 independent variables. The unstandardized coefficient beta of psychological risk ($\beta$ = -0.265) is interpreted when there is an increase of 1 unit of psychological risk, which will decrease 0.265 units of continual usage intention to use online banking.

The tolerance is the amount of variability of an independent variable not explained by other dependent variable. All variables have high tolerance value and don’t have multicollinearity problem because their tolerance value are > 0.19 as proven by such as privacy risk (0.293), financial risk (0.220), social risk (0.380), time risk (0.417), performance risk (0.318) and psychological risk (0.438). The findings indicate that privacy risk has no significant associated with continual usage intention of online banking (p= 0.217, $\beta$ = -0.085). This is probably because the respondents in this study understand and believe that banks in Malaysia can protect user’s personal and financial information when they transfer fund and transaction through online banking (Ling, Fern, Boon & Huat, 2016).

Furthermore, the findings from analysis disclosed that financial risk has no significant relationship with continual usage intention of online banking (p= 0.696, $\beta$ = 0.030). This result is in contrast to several findings in the literature which concluded that perceived financial resource
has significant affect to the behavioral intention to use online banking (Luarn & Lin, 2005). This is because, online banking in Malaysia is well developed and banking transactions are operated within the transparency.

Time risk was found to have negative significant relationship associated with continual usage intention of online banking (p= 0.002, β= -0.195). The previous studies also found that time risk has a significant relationship that influence the preferential factor to use internet banking (Singhal & Padhmanabhan, 2008). According to Yang et al. (2015) time-conscious users are likely to prevent the risk of time loss because they choose online transaction for the sake of convenience and time-saving.

The study also found that performance risk has no significant and negative associated with continual usage intention of online banking risk (p=0.154, β= -0.096). Prior research has found that performance risk was less salient to determine the behavior intention to use online banking service (Martins, Oliveira & Popović, 2014). The finding revealed that psychological risk has negative significant relationship to continual usage intention of online banking (p= 0.000, β= -0.265). Based on Yang, et al. (2015) which state that the overall risks such as security, financial, time, performance and social risk affect user’s uncertainty to the system and influence users’ anxiety, which called the psychological risk.

5. Conclusion

In conclusion, the psychological risk was found to have the biggest impact on the user’s continual usage intention of online banking. The bank recommends to implement training programs to improve the customer service function to eliminate only doubts and perceived risk by the user. Time risk was the second strongest negative factor. The bank should improve the performance and quality of online banking by hiring technical expertise to monitor the security system regularly in order to prevent online banking service from malfunction and error. Future research recommends that the future researcher can apply the other model or theory to determine user’s behavioral intention to continue using online banking in Malaysia such as the Theory of planned behavior (TPB) and Unified Theory of Acceptance (UTAUT) which are recommended for implementation for future research.

References


