

Internet Banking Security Guideline Model for Banking in Thailand

M.L.Kulthon Kasemsan and Nantana Hunngam

Faculty of Information Technology, Rangsit University, Pathumtani, Thailand

Abstract

The purpose of this research is to study the Internet banking security guideline model for banking business in Thailand. At the present, the uses of the Internet have grown rapidly, but there are not many customers who use the Internet banking services because they do not trust the bank security systems. As a result, the study of the Internet banking security guideline model and tools development as well as information technology were conducted to ensure the security of the Internet banking services by using the concept of reliability, innovation adoption theory, the quality of the Internet connection and e-commerce law. The collected data were taken to form the Internet banking services security model by using innovation adoption theory, trust of the system, the quality of the Internet connection, e-commerce legal support, authentication theory, key locker security, and one time password (OTP). The results of the research showed that the customers paid attention to the security, risk awareness, ease of use, and quality of Internet connection, respectively. Furthermore, it can also be concluded that a comparative study between the Internet banking and mobile banking should be studied as well as the study of social factors, and security factors to ensure the security and in order to meet with the customers' needs.

Keywords: Internet banking services, Internet banking security

Introduction

Nowadays, information technology takes the task of supporting and raising service efficiency in all businesses. Banking industry is one of the businesses that have brought IT to help with banking transactions and expand bank service opportunities to its customers. It conforms to the needs of modern society that the Internet plays an important role in people's daily life in general. It is also convenient for customers who usually use the Internet.

Advanced information technology has become one of the tools that many customers

can access to the Internet banking services easily and quickly by using IT. It can also decrease the crowd at bank counters as well as at the ATM's (Samphanwattanachai, 2007).

At the present, the uses of Internet banking services have grown slowly because many users worry about its service systems will not work as expected and trust of the system which is a crucial factor related to unwillingness to adopt service via the Internet (Rotchanakitumnuai, 2004). The security of services and the safety of customers' sensitive information are the main reasons in enhancing the efficiency of

the Internet banking services to gain customers' confidence. In order to attract more customers in the future and to be able to meet their specific needs, it is very important to study the Internet banking security guideline model and identify possible problem related to its services.

Research Framework

Trust of the System

Trust of the System: Strong concern about security is one crucial factor related to unwillingness to adopt service via the Internet. The results from research about Internet banking also reveals that security is one of the most important future challenges for banks because of customer fears of higher risk in using the web as a channel for financial transactions (Saadullah, 2007).

Turban concludes that security, reliability, perceived risk, responsibility, and customers' distrust appear to be the reasons why customers mistrust banking transactions. To find out how to win the customer's trust, an additional research in terms of trust element has been conducted by Saadullah (2007). The study has concluded that banking transactions should reinforce the following requirements as to gain customers' confidence:

- **Security:** Security appears to be an important factor related to mistrust in the Internet banking services. Security violations can cause various problems including the breakdown of operating system or prevent access to the information, and customers do not trust the security infrastructure on the Internet. Security is a very important factor for customers to adopt Internet banking services.
- **Reliability of Transaction:** Reliability refers to the efficiency and the ability of a system to perform its functions accurately, especially a foolproof system that can work properly. Making a system to perform its functions accurately and precisely, a dependable of

document issuance of banking transactions should be considered, thus providing an ability to keep all banking transactions' information accurately and can serve at a specific time.

- **Perceived Risk:** Perceived risk can cause users to reject new services of the Internet banking. In terms of perceived risk towards reliability and a system breakdown, users are worried that Internet banking service systems will not work as expected, and lack confidence that problems can be solved quickly. It is also found that transaction risk occurs when online markets fail to assure that service will be delivered with adequate quality. Frequently, slow response time after the Internet interaction leads to a delay of service delivery and causes customers to be unsure that the transaction was completed. The results of the study can adopt to support a research on perceived risk.
- **Slow Response Time:** Response time is a term associated with a willingness to help users and provide services promptly including sending an e-mail attached with banking transactions' receipt, calling back to users quickly and offering services in time, respond to users in a timely manner as well as an ability to provide the right and appropriate information to users when problems occurred. In addition, there is such a mechanism to deal with users' feedback and a banking transactions' guarantee.
- **Privacy:** Privacy is very important to the trust of a system. It is used as an indicator to ensure that users' information would not be taken out to exchange or use in an illegal way. Security is the most important feature in terms of quality in banking transactions. When security violations occur, there will be a problem of losing privacy as well. It appears to be a major cause as using various services on the Internet, which users do not have confidence in privacy's policy to help prevent unauthorized access to their confidential information.

Technology Acceptance Model (TAM)

Over the past ten years, there were many studies on the scope of investigation which approach to an acceptance of information technology and information system. Among the results from several studies on the presentation and examination about TAM, it seems that the study conducted by Davis in the year 1989 has emerged clearly to be an explanation process of information technology and information system. It can be concluded from the TAM that usefulness and ease of use of information technology and information system are two main factors which were adopted for all organizations to support usages and move along with the specific usages based on the usage and usefulness for all usage behavior as said above (Davis, 1989).

TAM based on Theory of Reasoned Action (TRA), and afterwards was developed to be Theory of Planned Behavior (TPB). According to TAM, it is can be assumed that the acceptability of an information system in organization is determined by two main factors: Perceived usefulness and Perceived ease of use. Those two factors are determined by the person's attitude towards the use of the system, behavioral intention to use, and actual system use.

Perceived usefulness (PU) is defined as being the degree to which a person believes that using a particular system would enhance his or her job performance.

Perceived ease of use (PEOU) refers to the degree to which a person believes that using a particular system would be free from effort related to a characteristic of a particular system such as smoothness, ease of use, ease to learn, and flexibility.

Security System Concepts

Nowadays, system security and protection is very important to organizations due to increasing treats from some programs and can cause extreme damage to organizations.

Hence, if the system has a better security control, the risks of threats would be reduced. Basic knowledge of authentication is an important step of security control. Authentication is any process by which you verify that a person is who claims he is and has been permitted to access to a system. Authentications used in this study are as follows:

- **Authentication:** Authentication is the process of confirming the identity of a person. In practice, there are 2 steps as follows:

Identification is a process of identity; something that identifies users such as a username.

Authentication is a process to verify that users are authentic which can be process as the following: In the first step, users will show evidence used in authentication to the system.

This step is called identification. In the following step, the system will verify evidence which is claimed by users and is known as authentication. After verification is completed, if evidence claimed correct, users are allowed accessing to a system but if not, users would be rejected (Jitcharoentham, Panchan and Limwiwatkul 2004).

Authentication by Password Authenticators or Tokens: A token is a small electronic device designed to give out a one time password (OTP) to be used as an access for online monetary transaction. A microchip embedded in the token stores countless sets of security code, and is clock-synchronized with bank server to generate a set of pass code. This code set is individually customized for different user. With a press on its button, a token will display six digits number. This code must be used as an OTP to gain access to user's online financial transaction every time. As long as you have your token in your pocket, the risk of being intruded or hacked will reduce dramatically since the Internet Banking will allow no

transaction without OTP code. The bank will send the token to mailing address indicated in your registration. You can start using your token by visiting your bank website to activate your token first.

Authenticator or a Token is a hardware that is used to create a dynamic password when logging into the network system. The authentication can be done in 2 types - Synchronous Authentication and Asynchronous Authentication.

1) Synchronous Authentication is available in 2 types according to type of usage.

Event-Synchronous Authentication:

When a user want to access to the system, a user must press the token to create a password. As a user inputs the password to the form to access to the system, the system then identifies with the server to check whether the code does exist in the server. Then the permission to access the system is granted.

Time-Synchronous Authentication:

In this method, password will be generated according to period of usage time. Normally the password will be changed in every one minute. As the system keeps generating passwords, some of them might be repeatedly created. To access to the system, a user needs to input both password generated by the token and the time that the password is created to the form. The system then checks whether time and password are correct and match before allowing the user to access to the system.

2) Asynchronous Authentication is also called Challenge-Response. It has been developed since the dynamic password was in it early state of development. The dynamic password is the most secured identification method. When a user attempts to access to the system, he will need to send request to a server. Then the server sends challenge string for the user to input in a token. The

token then generates password for users. With this password, a user can enter the system.

- A One-time Password Authentication (OTP): A one-time password is generated and developed to avoid a number of shortcomings that rise from repeated password usage. A one time password will make the system more secure because passwords will changes after each login: when a user attempts to access to the system, they will need to send request to a server.

Then the server sends challenge string for the user to input in a hash function. A hash function then generates hash value response, users then sends that value back to a server. The system then checks the value by comparing with the value computed by the system itself. When the values match each other, then the permission to access the system is granted (Jitcharoenthom, Panchan and Limwiwatkul 2004).

- SMS Security: All SMS messages are encrypted with standard IA5 and SS7 during transmission from the mobile to the mobile operator. The SMS text is then encrypted again with the standard MD5 and sent to MPC via a secure VPN which is a secure connection between the two servers and users with MPC. In addition, SMS messages between the bank and the mobile operator contain no information which would give access to any account. (Black, Lockett, Winklhofer and Mckechnie 2002).

There are two supporting factors that have been added to this study including quality of internet connection as in a study of Pikkarainen, Karjalouto and Pahnila (2004), and they have examined it in the form of Internet banking acceptance in Finland. It brings about acceptance or rejection to use online banking services. And another supporting factor is legal support from a study conducted by Rotchanakitumnuai (2004), which investigated corporate customer perspective on business value of

Thai internet banking. Legal support issues were adopted in this study.

Legal support has a great impact on users' internet banking acceptance as responsibility must be set when financial losses occur in Internet transactions. Thus, users have confidence to use online banking services. To gain the information associated with the actual facts and get the greatest results related to the hypothesis, the following two supporting factors have been added to a study:

Quality of Internet Connection

The importance of internet connection and the quality of signal have been used to interview the focus group as well as an access to the internet has been influenced towards usage of internet banking services. Without connecting internet properly, it is impossible to use online banking services (Pikkarainen, Karjalouto and Pahnla 2004).

Legal Support

Customer protection is a major legal issue associated with using the Internet. This issue can cover unfair and deceptive trade practices by service providers, unauthorized access, and usage by others. Customer protection is important for building customer confidence over the Internet. In addition, fair liability is a key legal issue (Rotchanakitumnuai, 2004).

Research Methodology

The related literatures have been reviewed to build a variable for a research framework

based on TAM included Perceived usefulness (PU), Perceived ease of use (PEOU), Trust of the System consist of Security, Reliability of Transaction, Slow Response Time, Privacy, and additional factors included Quality of internet connection and Legal support. In total, 400 users out of 2,320,000 internet banking users in Bangkok were purposively selected (National Statistical Office of Thailand, 2008)

The sample size was calculated using Taro Yamane formula at the confidence level at 95 percent and error at 5 percent. The hypotheses are as follow:

- H1: Perceived usefulness has positive impact on internet banking services adoption.
- H2: Perceived ease of use has positive impact on internet banking services adoption.
- H3: Quality of internet connection has positive impact on internet banking services adoption.
- H4: Legal support has positive impact on internet banking services adoption.
- H5: Trust of the System has positive impact on internet banking services adoption.

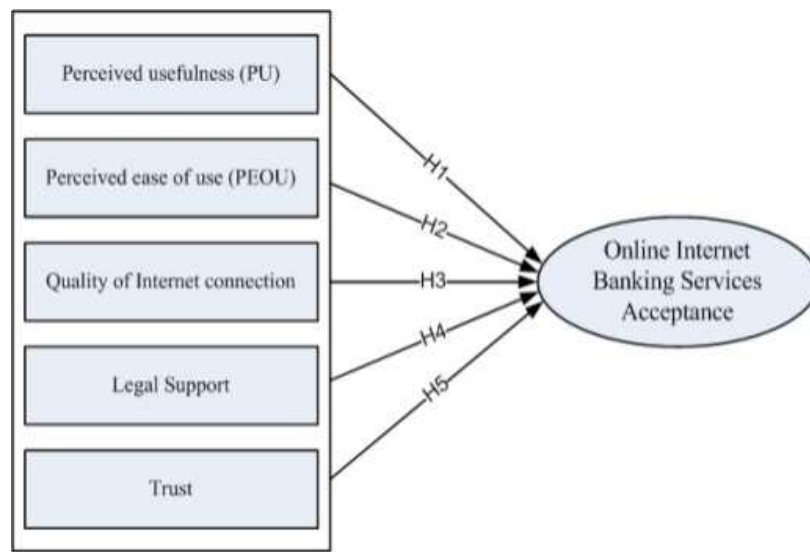


Fig 1. The Research Model: the Internet Banking Security Guideline Model for Banking Business in Thailand.

Research Tool

The instrument used to collect the data was developed in terms of questionnaire, constructed from related theories and various researches. To gain all information needed, the questionnaire content was divided into the following three sections:

- Section 1, contains 12 rating scale questions about innovation adoption to investigate the impact on the acceptance of innovation adoption.
- Section 2, contains 12 rating scale questions about the trust of the system consisted of security, reliability of transaction, perceived risk, slow response time, and privacy of Internet banking transactions user to investigate the impact on acceptance of the trust of the system.
- Section 3, contains 6 questions about the Internet banking security guideline model for banking business adoption. There are examples of various pages of usage in each step for users to choose the one they need. The information obtained from this section will be taken to form Internet banking

security guideline model for banking business.

The validity and reliability of constructed questionnaire were tested by the following methods:

- Content validity was tested by asking some advices from the experts to revise in order to form an appropriate questionnaire. The index of item-objective congruence was used in test development for evaluating content validity by five experts (Kitpreedaborisud, 1992). The index of item-objective congruence value is 0.95 that means they are congruence to each other.
- Thirty sets of improved questionnaire were tried out by the sample in order to measure reliability by using Cronbach's alpha coefficient. Alpha values result showed stability of questionnaire which its values between $0 < \alpha < 1$. The value that closes to 1 means questionnaire has high reliability (Davis, 1989). The set of questionnaire has reliability of 0.9.

Questionnaire data were analyzed by using SPSS program. The data were processed as follows:

- Descriptive Statistics are used to describe the features of a collection of data in each factor by percentage (%), and means.
- Inference Statistics by using Multiple Regression Analysis to examine the factors influenced on the acceptance of internet banking adoption including Perceived usefulness, Perceived ease of use, Quality of internet connection, Legal support, and Trust of the System whether they have a positive

impact on acceptance of Internet banking transactions or not. The obtained data were taken to determine the Internet banking security guideline model for banking business.

Findings

Descriptive Statistic Results

Analyses of the data involved the perspective on the need of Internet banking security guideline model for banking business, the collected data including data surveyed from the samples. The findings showed that:

Table 1: Level of Internet Banking Adoption

Level adoption of Internet banking	Mean	SD	Interpretation
1. Perceived usefulness (PU)	4.10	0.67	Extremely likely
2. Perceived ease of use (PEOU)	3.93	0.79	Quite likely
3. Quality of Internet Connection	3.92	0.78	Quite likely
4. Legal Support	3.68	0.82	Quite likely

As shown in Table 1, it was found that the respondents had a high level of confidence on internet banking adoption. When considered in each aspect, it was found that in term of PU, was rated at a "highest" level by means 4.10; followed by PEOU; Quality of internet connection; and Legal support were rated at a "high" level at 3.93, 3.92, and 3.68, respectively. It can be concluded that PU affects the use of Internet banking services as it reduces time at the bank counter and raises the services performance. PEOU affects the use of Internet banking services as it has procedure that is easier than using services over the bank counters, available 24

hours a day, and easy to understand, Quality of internet connection affects the use of Internet banking services as the speed of the Internet can help using services continuously and it can also guarantee that services are completed every time, and Legal support affects the use of Internet banking services as it has the personal information protection and e-commerce law to prevent unauthorized access to users' confidential information. It is a supporting law about electronic documents as legal evidence of transactions to ensure that the users will be protected when a problem occurs.

Table 2: Level of Trust on Internet Banking Adoption

Level adoption of Internet banking	Mean	SD	Interpretation
1. Security	2.89	0.93	Slightly likely
2. Reliability of Transaction	3.67	0.69	Quite likely
3. Perceived Risk	3.82	0.77	Quite likely
4. Slow Response Time	4.00	0.85	Quite likely
5. Privacy	3.89	0.69	Quite likely

As shown in Table 2, it was found that the respondents had a high level of confidence on internet banking adoption. When considered in each aspect, it was found that in term of Slow Response Time, Privacy, Perceived Risk, and Reliability of Transaction were rated at a "high" level at 4.00, 3.89, 3.82, and 3.67, respectively. In terms of Security, it was rated at a "moderate" level at 2.89. It can be concluded that Security affects the usage of Internet banking services as users worry about Phishing, Trojan, Key Logger, and public computer, Reliability of Transaction affects the usage of Internet banking services as users' need transactions report periodically to prevent access from others and report from the bank whether the transaction was completed or not in order to reduce redundancy of transactions. In terms of Perceived Risk, it was found that it affects the usage of Internet banking services as users need to use OTP and limit the amount of money in transaction to reduce the risk of transaction. Privacy affects the usage of Internet banking services as users do not have confidence to do transaction via public

computer or other devices and they also do not have confidence whether sending Information through SMS message via mobile phone is secured or not. And in terms of Slow Response Time, it was found that it affects the usage of Internet banking services as users need the bank to verify the amount of transaction in each time by using the second password for authentication in order to increase security and confidence to use the internet banking services.

Regression Analysis

The hypotheses were tested by using Multiple Regression Analysis to examine the factors influenced on the acceptance of internet banking adoption including Perceived usefulness, Perceived ease of use, as well as Quality of internet connection, Legal support, and Trust of the System have a positive impact on acceptance of Internet banking transactions as shown in Table 3 and 4.

Table 3: Regression Analysis Results of Each Factor for the Effects on the Acceptance of Internet Banking Adoption in Bangkok

Variables Entered	Unstandardized Coefficients		Standardized Coefficients	t-test	P-value
	B	Std. Error	Beta		
Constant	0.046	0.280	0.00	0.165	0.869
Perceived usefulness(PU)	-0.146	0.077	-0.126	-1.906	0.057
Perceived ease of use (PEOU)	0.307	0.076	0.277	4.059	0.000
Quality of Internet connections	0.161	0.065	0.143	2.490	0.013
Legal Support	-0.070	0.056	-0.064	-1.233	0.218
Trust of the system	0.458	0.079	0.305	5.795	0.000
F- test = 24.751 P-Value = 0.000					
Standard Error of the Estimate = 0.777					
R = 0.490					
R Square = 0.240					
Durbin-Watson = 1.530					

As shown in Table 3, it was found that the five factors have influenced on the acceptance of internet banking adoption had statistically significant difference at 0.05 ($F=24.75$ $P\text{-Value}=0.000$) associated with the usage of internet banking transactions 49 percent ($R=0.49$). The variation of the usage of internet banking transaction will be varied 24 percent ($R\text{ Square}= 0.240$) depending on the five factors. And the autocorrelation was not associated with the time ($\text{Durbin-Watson}=1.530$). When considered in each

factor, it was found that PEOU, Quality of internet connection, and Trust of the System have influenced on the usage of internet banking transaction had significant difference at 0.05. The variation of PEOU, Quality of internet connection, and Trust of the System 1 unit can change the degree of e-commerce transaction usage 0.307, 0.161, and 0.458, respectively. The Trust of the System divided to five factors shown in Table 4.

Table 4: Regression Analysis Results of Each Factor for the Effects on the Trust of the System to Use Internet Banking Transactions in Bangkok

Variables Entered	Unstandardized Coefficients		Standardized Coefficients	t-test	P-value
	B	Std. Error	Beta		
Constant	0.609	0.282	0.00	2.159	0.031
Security	0.287	0.054	0.303	5.312	0.000
Reliability of Transaction	0.023	0.072	0.018	0.319	0.750
Perceived Risk	0.272	0.065	0.238	4.162	0.000
Slow Response Time	0.008	0.055	0.008	0.148	0.883
Privacy	0.010	0.050	0.011	0.201	0.841
F- test = 19.087 P-Value = 0.000					
Standard Error of the Estimate = 0.800					
R =0.442					
R Square = 0.196					
Durbin-Watson=1.495					

As shown in Table 4, the Trust of the System which is divided to five factors have influenced on the usage of internet banking transactions had statistically significant difference at 0.05 (F=19.09 P-Value = 0.000) associated with the usage of internet banking transactions 44 percent (R=0.44). The variation of the usage of internet banking transactions will be varied 20 percent (R Square= 0.196) depending on the five factors. And the autocorrelation was not associated with the time (Durbin-Waston = 1.495). When considered in each factor, it was found that Security and Perceived Risk have influenced on the usage of internet banking transactions had significant difference at 0.05. The variation of Security and Perceived Risk 1 unit can change the degree of e-commerce transaction usage 0.287 and 0.272, respectively. As the results from hypotheses tested found that the factors that have negative impact on the usage of Internet banking services were as follows: PEOU affects the use of Internet banking services as

it has procedure that is more convenient than using services over the bank counter, available 24 hours a day, and easy to understand; Quality of internet connection affects the usage of Internet banking services as the speed of the Internet can help using services continuously and it can also guarantee that services are completed every time. In terms of the Trust of the System, it was found that the following factors have negative impact on the usage of Internet banking services: Security affects the usage of Internet banking services; Reliability of Transaction affects the usage of Internet banking services as users' need transactions report periodically to prevent access from others and report from the bank whether the transaction was completed or not in order to reduce redundancy of transactions. In terms of Perceived Risk, it was found that it affects the usage of Internet banking services as users need to use OTP and limit the amount of money in transaction to reduce the risk of internet banking transactions.

From the results gathered from users' opinion, the Internet banking security guideline model was proposed as show on figure 2 by forming the Internet banking transactions model. It suggests that the Internet banking transaction should be ease to learn and use, the service procedure is not difficult and available 24 hours a day. It also suggests that the users should use the high

speed internet in order to use services continuously as well as use the authentication with key logger, prevent the username and password to log-in to the system by using additional devices that can generate dynamic password such as Safeword card or Token card, and provide handbook for safe log-in.

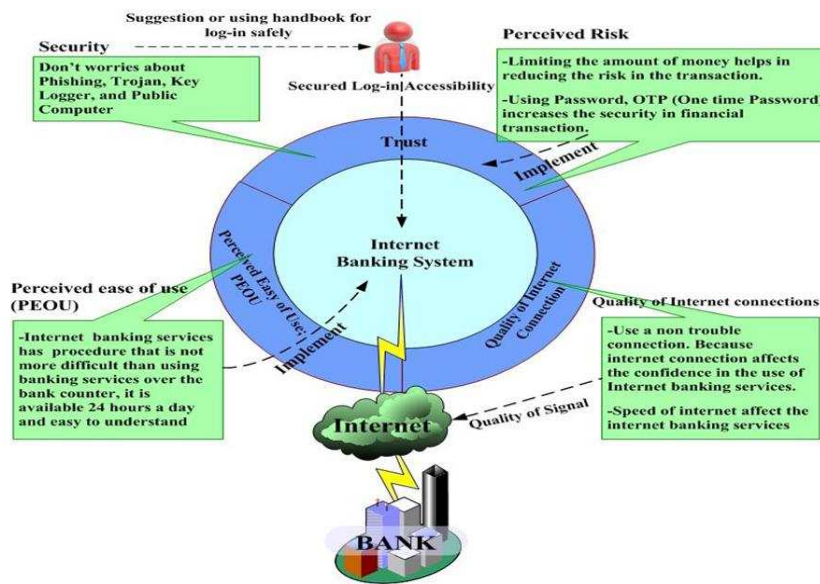


Fig 2. Shows the Internet Banking Security Guideline Model

As shown in figure 2, an inmost circle is Internet banking system. The following research results were taken to form Internet banking transactions model:

1. Perceived ease of use (PEOU) by implementing the obtained information to the system in order to make it easier to use.
2. Quality of Internet connections by suggesting the users that they should use the high speed internet in order to use services

continuously and the impact on trusty of using Internet banking services were reduced

3. Trust of the System:

- In terms of security, obtained information was taken to provide handbook for safety use of Internet banking services to prevent financial corruption as well as improving technology in order to prevent occurrences of transaction risk.

- In term of perceived risk, the amount of money in transaction should be limited which users can limit amount of money by contact the bank directly. A token was taken to give out a one time password and implement to the system to make it safer.

Conclusion

The study of the Internet banking security guideline model was conducted to ensure the security of the Internet banking services and increase the usage of the Internet banking services.

The results of the research showed that the following factors have influenced on the usage of Internet banking transactions: PEOU, Quality of internet connections, and the factor of confidence to system as well as the Trust of the System including Security and Perceived Risk.

Details of each factor were taken to form the Internet banking security guideline model which is easy to learn and use, and available 24 hours a day.

It also suggests that the users should use the high speed internet in order to use services continuously as well as authentication by using device that can generate dynamic password during the specific time to prevent usage of password twice, limit the amount of money in transaction and verify financial amount that exceeds an amount of money limited to prevent financial corruption.

In addition, the banks should send SMS message through mobile phone to assure an access to the system and usage of various services on the Internet as it will be the services evidence that can prevent financial corruption in case of transactions done by others. Finally, handbook for safe log-in should be provided to the users. The results from the investigation on users' perspective towards the usage of internet banking transactions meet all the present research hypotheses. Further research should investigate users' perspective towards the usage of internet banking transactions compare with the usage of mobile banking transactions and security factor. Gaining the

results precisely from a research on the usage of internet banking transactions may help create strategies to enhance and improve services' performance, so a particular bank should be selected to start another study.

References

Black, N. J., Lockett, A., Ennew, C., Winklhofer, H. & Mckechnie, S. (2002). "Modeling Consumer Choice of Distribution Channels: An Illustration from Financial Services," *International Journal of Bank Marketing*, Vol. 20 No. 4, 161-173.

Davis, F. D. "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology," *MIS Quarterly*. 13, 3. (1989): 319-340.

Jitcharoentham, S., Panchan, S. & Limwiwatkul, L. (2004). "Introduction to Authentication," [Online], [Retrieved December 29, 2009], http://www.thaicert.nectec.or.th/paper/authentication_guide.php

Kitpreedaborisud, B. (1992). "Teacher Handbook: Measurement and Evaluation of Teaching-Learning," *Bangkok: B&B Publisher*, 2nd Edition.

Modernform Integration Service, (2009). "Access Control," [Online], [Retrieved December 29, 2009], http://www.misco.co.th/Solutions_products/Access_Control_andAuthentication_Solution.html.

National Statistical Office of Thailand (2008). "The Total of Having and Using an Information Technology (households)," [Online], [Retrieved December 29, 2009], <http://www.service.nso.go.th/nso/nsopublish/service/survey/IctHRep51.pdf>

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H. & Pahnla, S. (2004). "Consumer Acceptance of Online Banking: An Extension

of the Technology Acceptance Model," *Internet Research*, Vol.14, No.3.

Rotchanakitumnuai, S. (2004). "Corporate Customer Perspectives on Business Value of Thai Internet Banking," *Journal of Electronic Commerce Research*, Vol. 5, NO. 4.

Saadullah, K. (2007). 'Adoption Issues of Internet Banking in Pakistani Firms,' Master Thesis, Computer and Systems Science, Department of Business Administration and Social Sciences Division of Information Systems Sciences, Luleå University.

Samphanwattanachai, B. (2007). "Internet Banking Adoption in Thailand: a Delphi Study," Preceeding of the 24th South East Asia Regional Computer Conference. Bangkok: November 18-19.

Wanitbuncha, K. (2006). "Using SPSS for Windows in Data Analysis, Bangkok: Chulalongkorn Book Center," 8th Edition.