EVALUATION MODEL FOR SECURITY COMPONENTS: A CASE STUDY ON MALAYSIAN INTERNET BANKING

ABSTRACT. The usage of Internet Banking in Malaysia, which started about 10 years ago, has been well accepted by consumers. Statistics from Bank Negara Malaysia (BNM) show that every year there is an increase in the number of registered individual Internet banking users since its inception in Malaysia. As at the third quarter of 2010, there were approximately 9.2 million registered Internet Banking users compared to only 2.6 million in 2005. A survey of 264 CIMB Bank Berhad personnel revealed that although there is a high degree of confidence, with respondents claiming to be aware of requirements by the bank, further and thorough inspections suggest that there are several areas in which desirable knowledge and understanding are still lacking. Additionally, in order to identify the currents state of the security features offered, we performed an analysis of six (6) Internet Banking websites in Malaysia. Using the evaluation model proposed in this study, an analysis of Internet banking website security elements revealed that there is still room for improvement in areas such as helping users to execute transactions and create awareness on their responsibilities as outlined by the banks.

INTRODUCTION

There has been many studies concerning Malaysia's online banking security and usability which focus on service quality evaluation (Vijayan and Bala Shanmugam, 2003) and user acceptance of such facilities (Yuen and Yeow, 2009; Khalil and Pearson, 2007). As such, there is a need to conduct a study in this area that will develop an evaluation model for examining the current state of security features available on Malaysia's Internet banking websites. In addition to this, it is important to examine whether the Internet banking users' in Malaysia are complying with the security requirements set by major Malaysian banks.

LITERATURE REVIEW

Security and Threats in Internet Banking

It cannot be denied that security plays a vital role in internet banking as it involved monetary transaction. Studies performed by (Mattila and Mattila, 2005; Centeno, 2004; Yiu et al., 2007) concluded that security is always been seen as the main service barrier to the internet banking as it affects in the user acceptance towards such facilities.

Rapid development of internet banking capabilities carries risks as well as benefits. Since the early implementation of internet banking, most of the studies highlighted that the lack of trust and privacy that is obtaining, distribution or non-authorized used of personal information are well-known risks posed by internet banking. Yet, as the technology and people are getting

more creative, the threats of internet usage have been extended to various means i.e. user terminal/user (e.g. user surveillance, theft of token, phishing, token attack tools, and malicious software installation); communication channel (e.g. pharming, sniffing, session hijacking) and internet banking server (e.g. brute-force attacks, website manipulation and bank security policy violation).

Evaluation Technique – Cognitive Walkthrough

The main objective of this study is to develop an evaluation model of the security components for local internet banking websites. Hence, it is important to explore the available techniques used in evaluating the websites. Cognitive Walkthrough (CW) is one of the evaluation techniques available other than heuristic evaluation. CW is familiar in human-computer interaction (HCI) as a tool to improve interface usability. CW is a methodology for executing the theory-based usability evaluations of user interfaces. In CW, evaluator will focus on the user's goals and actions as well as the system affordances that support or deter the effective accomplishment of those goals. The evaluator evaluates the user interface by examining the cognitive processes required for achieving the goals set (Wharton et al., 1992; Jaspers, 2008). Unlike heuristic evaluation, CW is highly structured and clearly guided by user's tasks.

This methodology has been chosen as the evaluation technique due to the objectives of the CW which focuses on the user's goals and actions as well as the system affordances that support or deter the effective accomplishment of those goals. This method has been used by (Mannan & Oorschot, 2007) and (Hertzum et al, 2004) in their study to examine internet banking security and usability towards Canadian and Denmark banks.

RESEARCH FRAMEWORK AND MODEL

Research Model

To provide a clearer picture of the overall research process involved in this project, we divided this research model into five phases with 3 different categories i.e. Phases, Actual Action and Deliverables as shown in Figure 1.

Phase 1 consists of a preliminary analysis which involves reviewing and synthesizing information obtained from articles published in established journals. All articles analyzed in this study were mostly related to current security issues in internet banking. It is important to note that, the security requirements, guidelines, usability criteria as well as evaluation techniques for the development of the evaluation model was determined in this phase. The aim of this phase is to develop a research methodology framework, which is based on the evaluation technique available. We named this framework as was called the Internet Banking Security Evaluation Framework (IBSEF).

In Phase 2, IBSEF was used as a guideline in evaluating the security and usability features available in six (6) internet Internet banking websites in Malaysia.

The Internet Banking Security Evaluation Component (IBSEC) Model developed in Phase 3 which was based on the literature review performed in Phase 1 and observation made during the analysis of the internet banking websites (Phase 2) above.

Phase 4 emphasizes the testing and validation of the IBSEC Model. In this phase, a survey will be conducted among banking personnel in CIMB Bank Bhd. to gauge the Malaysian habits and understanding of the usage of internet banking in terms of security. Finally, in the Phase 5, a detail work carried out in this study which also includes the limitation faced, overall recommendations in enhancing deficiencies found in analysis (Phase 1 and 2) and suggestions for future works are documented.

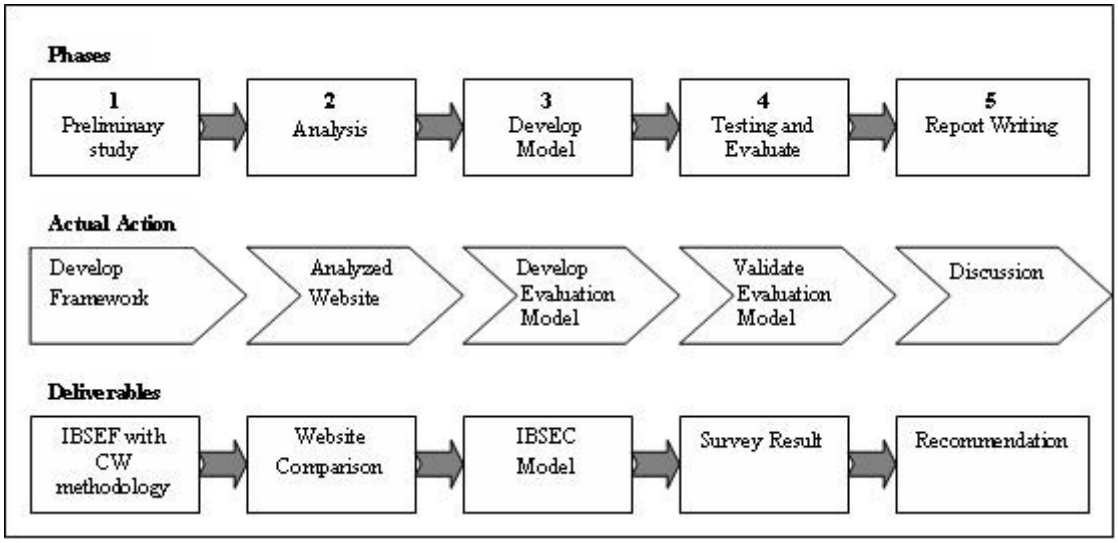

Figure 1. Research Model.

Internet Banking Security Evaluation Framework (IBSEF)

As shown in Figure 2, we proposed IBSEF based on Cognitive Walkthrough (CW) methodology.

The first phase of this framework specifies **Goals** that need to be accomplished. The goals in this context are all security elements have been implemented in the websites. Based on the studies performed for security in internet banking areas (Claessens et al., 2002; Zopolskia and Kotulski, 2007; Hutchinson and Warren, 2003; Wison, 1999), concluded that Confidentiality, Integrity, Auditability, Availability, Privacy, Authentication and Non-Repudiation are categorized as crucial and must be implemented to secure internet banking. Apart from assurance on security elements, internet banking websites also should provide awareness to educate users as stated in BNM Guidelines on the Provision of Electronic Banking Services.

The second phase is **Interface** and it is referring assessment of the acceptance of the design of the website use for Internet Banking. In this case, six (6) internet banking websites which comprises of three (3) local banks (Maybank, CIMB and Public Bank) and another there (3) foreign banks' (Citibank, HSBC and Standard Chart) internet banking websites were selected. The criteria of the selection of the internet banking websites were based on web traffic ranking analysis as at the month of September 2010 using the web traffic analyzer, Alexa Internet Inc.

In the third phase, i.e. **Selection of Action**, suitable evaluation methods and guidelines need to be identified in order to validate the effectiveness and susceptibility of the model. Two (2) BNM (Bank Negara Malaysia) Guidelines which related to managing of information technology and internet banking for financial institutions in Malaysia i.e. BNM Guidelines on the Provision of Electronic Banking Services and BNM Guidelines of Management of IT Environment (GPIS 1) will be used as a basis of this assessment.

The last phase i.e. **Perform Action** will be the execution on the activities/tasks which have been set in the previous phase. The details assessment activities checklist will be use in order to perform this analysis.

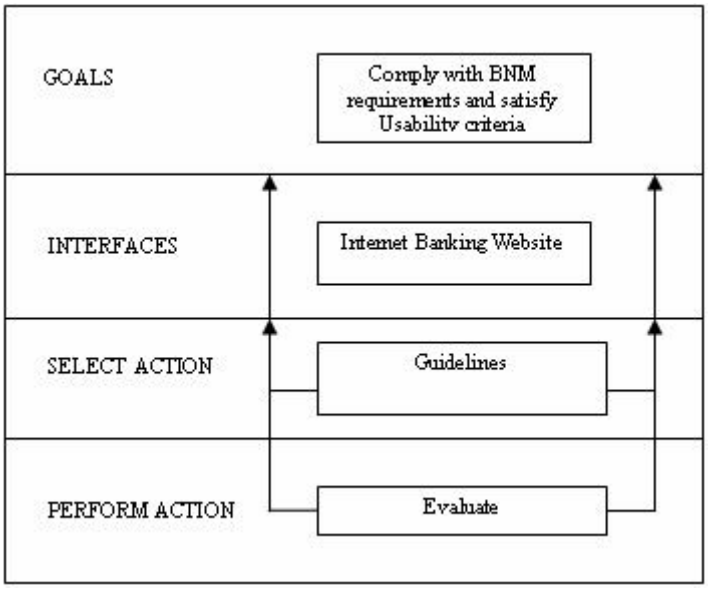

Figure 2. Internet Banking Security Evaluation Framework (IBSEF)

Internet Banking Security Evaluation Components (IBSEC) Model

Figure 3 below shows the evaluation model derived based on the observation during analysis towards six (6) internet banking websites in Malaysia. Overall study performed from the review of literature also helps in developing this model.

In this model, we identified three (3) important and inter-related components associated to the evaluation components in Internet Banking namely Security Components, Awareness and Usability components. The first component i.e. **Security** deals with the eight (8) security elements i.e. Confidentiality, Authentication, Non-Repudiation, Availability, Privacy, Integrity, Auditability, and Authorization which are compulsory in internet banking. The second components deal with the **Awareness**. The scope of awareness can be view from two angles i.e. banks initiatives in providing the security awareness to the users as well as the user itself whether they are aware with the internet banking risks and ways to eliminate or mitigate it. Finally is the **Usability** component. In order to highlight the usability issues in the implementation of the security posture in internet banking websites, the usability criteria i.e. Understandable, Locatable, Visible and Convenient, Speed, Ease of Use and Controllable were analysed. (Flavia et al., 2007) states that web site usability is a critical factor on the development of electronic commerce.

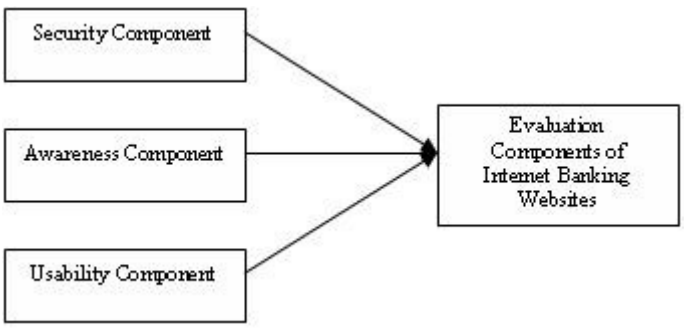

Figure 3. Internet Banking Security Evaluation Components (IBSEC)

Testing and Validation of IBSEC Model

The testing and validation of this framework is closely related to awareness attributes in Figure 3 above as it involve a survey to gauge an overview of the current situation of Malaysian local internet banking users' usage and knowledge in terms of security requirements set by major Malaysian banks. Three (3) variables were used in the survey questionnaire i.e. Computer Configurations, User's Practice as well as User Awareness.

In **Computer Configurations** variable, the end users knowledge in the usage and implementation of defense measures such as anti-virus, anti spyware, firewall and browser update are crucial in order to ensure their computers are securely safe. Establishing the end **Users Practice** or habits towards selection of operating system and browser, implementation of defense measures and the frequency of use of certain services such as P2P will assists us in identifying whether they are exposing themselves to the security threats during performing online banking transactions. **User Awareness** variable establish whether users are security conscious when it comes to password management and applying the internet banking best practices such as looking at closed padlock, SSL certificate and opening email from banks. By looking at users response to the proposed types of questions in PVQs can measure the users' alertness towards security in internet banking.

RESULT AND DISCUSSION

a. Analysis of security features in internet banking in Malaysia

Despite the fact that all local internet banking complies with Bank Negara Guidelines on Internet Banking, in terms of two-factor authentication (TFA) implementation and other security elements, the study shows that there are still lot of improvement needed to tighten the security measures. We discussed the deficiencies found and recommendations as below:

i. Authentication. Password remains the dominant means of authentication for the internet banking. This is may be due to their simplicity, legacy deployment and ease of revocation. As all aware, even though password can be transferred via secured channel, this common authentication approach is still vulnerable to online threats such as phishing, password stealing,Trojan via keylogger software along with installed malware or spyware as well as shoulder surfing. (Mannan and Oorschot, 2007; Coskun and Herley, 2008; Oorshot and Wan, 2009). SMS authentication is the most preferred types of two-factor authentication (TFA) by the local banks in Malaysia compared to other types such as types of authentication PVQs or token. HSBC provides two (2) types of login depending on types of transactions performed by users. As for normal transactions such as viewing account balances or transfer to own accounts (for example from savings account to current account), user is only needed to login with combination of username, password and secondary password. The combination of username, password and security code from token is needed when more risky transaction is performed such as transfer to 3rd party account, request for cheque book as well as updating personal information. Citibank implemented usage PVQ. During creation of internet banking ID and password, Citibank requires user to select three (3) out of ten (10) questions. Subsequently, one of the questions will be asked during user login to the system.

Banks recommend that password be unique, however only Citibank provides a high-quality password checking. In Citibank internet banking, system will prevent users from creating a password with usage of three (3) identical characters in a row such as 'alpha111' or 'aaa126', as well as usage of three consecutive alphabets or numbers in a row (e.g. abc269 or alpha123). Apart from that users are not allowed to create a username using their own name. These are very good features as this can protect users from creating a weak password and avoid attacker guessing on the username.

In term of password length, again, the foreign banks (Citibank and HSBC) are practising a very good approach of allowing up to thirty (30) characters in length. Longer password length would make difficult for attacker to guess the password.

Public Bank is the only bank among these six (6) banks that request their users to change the password on every 90 days. The numbers of users who have forgotten the current password may be increase if the banks activate the force change password (on monthly basis) feature. Bank may think that this could cause inconveniences to the users whereby they have to go through the re-registration process which include the getting e-pin at the automated teller machine.

As for the features to reuse of old password, Citibank, Maybank and StandChart take a brilliant decision for not allowing the old password to be reuse. This would help the tendency for the users to use same password which then would be easy for the attacker to guess the password. The feature for users to change the password is available on all of these six online banking systems. However, in terms of *visibility*, we found that Maybank has given a good example by putting it at the main screen and using a clear indication on where user can find a screen to change their internet banking password.

We would like to highlight that when compared between local and foreign internet banking websites, foreign banks do provide clear information on the steps involved online banking registration process. Besides, all of these three (3) foreign banking websites also provides quick tips or hint in the same page during creation of user name or password. These are the factors that we think addressed *visibility* and in way educate and reminded users of the importance to create a strong password.

ii. Bank's Authentication - These six (6) banks ask users to check or even type the URL of the bank website before entering the username and password. However, it is quite difficult for users to determine whether below URL login is correct or not. https://www.maybank2u.com.my/mbb/m2u/common/M2ULogin.do?action=Login.Misspelled login URL could cause users to be redirected to spoofed or malicious websites. A bookmarked login URL on the other hand, could be replaced by a phishing site URL by malware on a user PC. Nevertheless, CIMB Clicks do provide a memorable and simple login URL i.e. https://www.cimbclicks.com.my/ibk/

iii. Awareness - Banks also encouraged users to performed regular updates on security patches to OS and browser. Overall, these six (6) banks do provide links to the browsers and OS official websites to look for most updated security features available. However, upon checking to the links provided by Maybank and CIMB Clicks on Netscape and Windows linkage, we found out that the websites is no longer exists or cannot be found.

Apart from that, banks also encouraged users to performed regular updates on security patches to OS and browser. Overall, these six (6) banks do provide links to the browsers and OS official websites to look for most updated security features available. However, upon checking to the links provided by Maybank and CIMB Clicks on Netscape and Windows linkage, we found out that the websites is no longer exists or cannot be found.

In terms of usability, to perform a proper installation and maintenance of updating OS, browser, firewall and anti-malware would require person with technical expertise, which is quite challenging for many average computer users. Performing patches activities to OS and browser also bringing troublesome to the users. (Mannan & Oorschot, 2007) concludes that "patch management includes collecting all necessary patches, dealing with post patch conflicts, determining the trustworthiness of a patch source etc".

Even though these six banks indicate the importance to look for SSL padlock, Citibank informed user of Internet Explorer (IE) should look the locked padlock icon on the bottom right of the status bar, which is already outdated for IE 7 and 8. CIMB Clicks on the other hand

inform user to look for the closed padlock on the browser chrome which is not applicable for Firefox browser. This will create confusion especially to non-IT literate users.

Arising from the problem on fake certificate, we think that users should be informed on how to perform such validation checking and what are the important items to look in the SSL certificate. In this case, only Public Bank explained on how and what to check for validity of the SSL certificate.

Among these six (6) banks, CIMB Clicks, HSBC and StandChart does provides informative and useful awareness on phishing with samples of phishing websites, bogus email and steps to avoid being a victim and actions to be taken if users feel that they have been a victim of the phishing scheme. Besides, they also provide details explanation on terms related to phishing as well as phishing modus operandi. Common internet banking scams terms such as Phishing Mule, Nigerian Advanced Fee Scheme, Email Hoax are also been explained in the page. StandChart go step beyond by explaining on another types of online threat i.e. Vishing.

iv. Online jargon - StandChart and HSBC has provided users with a very good approach in ensuring users understand the contents of internet banking by providing and glossary and online jargon translation on the website.

b. Survey Analysis

The respondents for this survey were divided into 2 categories i.e. from IT and Non-IT background of work. Based from 264 questionnaires gathered, eighty percent (80%, N = 225) of the respondents are the internet banking users. Out of 264, (15%, N = 39) respondents who are not the users of internet banking stated that the main reason for not using this facility is related to trust.

The results of the survey is rather alarming, as most of the respondents do not complies with bank's security requirements as stated in the Internet Banking term and conditions. There are certain areas which still require more attention. Below are the details:

i. End user's computer configurations - Usage of secure web browser is crucial in performing internet banking transaction. Web browser vulnerabilities are commonly exploited when the user visited malicious websites. "IE6 has been reported not to be considered as the most secure version of IE" (Frei at all, 2007). In this survey, most of the respondents reported that they do keep their browser up-to date (67%, N = 152) however, we found that more than half of the respondents used IE with highest percentage in IE6 (33%, N = 74%). This shows that the respondents do not use the latest secure browser version as recommended by the banks and we believe respondents are over-reported on keeping with the browser up-to date status. In terms of operating system, Windows continues to be the most popular type operating system used by most of the respondents with higher percentage in Windows XP. Even when Windows was theoretically at its worst with regards to security compared to Linux, by having secure configurations and equipped with good anti-malware tools could reduce the risks of computer being attacked.

ii. End user's habit and practice – Most of the respondents do applied automatic updates mechanism to OS, browsers, firewall and anti-malware to the computer systems. This may due to fact that, the respondents is performing the online banking transaction in the office, in this case is bank itself.

Apparently most respondents do not follow the frequent password change recommendation by the banks, as only (14%, N = 32) out of 225 respondents reported changing their password on a monthly basis. This could be one of the impacts of the bank for not enforcing users to change the password.

iii. User awareness - (35%, N = 79) out of 225 of the respondents informed that they do read the banking agreement, privacy and security policies, we believed most of them do not really

go through the contents of the agreement. First, is because the nature of the agreement which is too lengthy, that caused users to ignore to go through it. Second, security is taken for granted, at least until individuals experience major drawbacks from the lack of security in their personal life. Note that except Citibank, the other five (5) banks have more than 2000 words in their terms and condition agreement. (Good et al., 2007) stated that "most users don't bother to read the lengthy and legalistic End User License Agreements".In terms of using a unique password, even though we could see higher percentage of the respondents (78%, N = 175) comply with bank recommendation, we could not determine the effectiveness of the password used. Some of the respondents might have used their name combined with their birth date or just their name ending with '123', just for the sake of letting the system accepting user's chosen password. Do take note that 100% of the respondents listed are using local bank's internet banking. According to our analysis, local internet banks only perform checking for usage of alphanumeric, not the complexity of the password as what Citibank did.

BNM Guidelines on Provision of Internet Banking clearly announced that bank will not send any email requesting for IDs and passwords as well as for verification purposes or even announcement on technical problems in the system. However, still there are number of the respondent state that they have received an email from banks to update personal data via the link provided in the email and out of (40%, N = 89) respondent, (5%, N = 12) responded to the email.

(89%, N = 200) of the respondents agreed with the implementation of PVQs in internet banking as to improve the security and mitigate the online risks. The main reason of (11% , N = 25) of the respondents who do not agree with the implementation is because PVQs are still not secure enough as attackers would still be able to guess the answers and easily obtained the information via social engineering. As expected, the question on 'What is your mother's maiden name' is still popular question chosen (26%, N = 142), followed by 'Favourite colour' (19%, N = 103). Several studies concluded that "Mother's Maiden Name?" is no longer suitable to be used in PVQs (Griffith and Jakobsson, 2007). As for "Favourite color", it will be at high risk of attack, as the answers possess very limited entropy. Most of the respondents replied 'Easy to remember' as their reason on the selection of PVQs questions.Finally, it is good to know that high percentage of respondents following bank's recommendation to look for the browser's basic security indicator (look for https, logout after complete online transaction and look for closed padlock. However, in reality several experiments performed by for example (Dhamija et al, 2006; Herzberg and Jbara, 2004) proved the other way round.

CONCLUSION AND FUTURE WORK

As illustrated in Figure 3, IBSEC consists of three (3) components i.e. Security Components, Awareness and Usability Components. Based from the analysis performed, it is clearly shown that these three (3) components are crucial in any implementation of 'perfect' internet banking. **Security** components portrayed the importance of having a secured system being served to the users. This resulted in increased consumers' confidence on the usage which in turn, giving benefits to the banks in terms of charges as well as reduction in operating costs (staffs and physical branch). Even though the result of the survey is rather alarming, looking from a positive side, it shown that most of the respondents have higher level of awareness of the security requirements set by banks. **Usability** components contribute to the increase of the **Awareness** level of the users. Usage of correct terms and placement of proper functions, clear instructions, having an updated user awareness message, usage of online technical jargon, simple, understandable and yet comprehensive terms and condition agreements justify the statement. The relationship between Usability and Security has been always known for its natural trade-off (Chellappa & Sin, 2005).With the model proposed in this study, it is expected that **Awareness** components could resolve **Usability** and **Security** issues. For example, by having effective awareness given to users (usage of alphanumeric, symbols, upper and

lower case alphabet) plus with the enforcement from the system itself, users would know and realized the on importance of creating secure password.

The framework proposed helps to develop a better approach in evaluating the security components for local internet banking websites. This study also highlighted how far internet banking websites helps users in giving out the security awareness and how far users understand and apply the security knowledge while performing the online banking transaction. Banks can use the result of this study as a reference that proactive actions should be taken in ensuring the users understand on their responsibilities in performing the online banking transactions. Not only on the product marketing, bank's websites should also emphasizes and creative in promoting security awareness to the customer. In addition to that, banks together with Cyber Security and Malaysian Communications and Multimedia Commission (MCMC) should formulate a programme at national level. One (1) respondent suggested that banks to conduct a free awareness briefing to the internet banking users as part of the programme. We think this is a good suggestion as other than creating a good relationship with customers, it will build a good image of the bank. Ultimately, the customer's trust would also be increased.

The following suggestions in regard to future research are either extensions to the current study or are the information gaps in the current literature review:

i. Future studies should emphasize on what are the most effective security awareness should be performed not only to internet banking user, but also to other alternatives banking methods such mobile banking.

ii. The same evaluation method could be implemented to other new methods on electronic banking such as mobile banking to evaluate how far users comply with requirements by the banks.

iii. Study on HCI especially in security and usability field which involves Malaysian residents can still be considered new compared to other countries; hence more concentration should be given to this.

REFERENCES

Chellappa, R. K., & Sin, R. (2005). Personalization versus Privacy : An Empirical Examination of the Online Consumer ' s Dilemma. *Information Technology and Management*. 2005:181-202.

Claessens J., Cock V. D. D. D., Preneel B., Vandewalle J. (2002). "On the Security of Today s Online Electronic Banking Systems", Computers & Security, Vol 21, No 3, 2002, pp. 257-269.

Centeno C. (2004). Adoption of Internet services in the Acceding and Candidate Countries, lessons from the Internet banking case, Telematics and Informatics, vol.21, no.4, February, 2004, pp. 393-315.

Coskun B, Herley C. (2008). Can "Something You Know" Be Saved? 2008:421-440.

Dhamija R, Tygar JD, Berkeley UC, Berkeley UC. Why Phishing Works. *Knowledge Creation Diffusion Utilization*. 2006;(November 2005):581-590.

Flavia C, Guinal M, Casalo LV. The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*. 2007;31(5):583-603.

Frei S, Duebendorfer T, Ollmann G, May M. Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the "insecurity iceberg " Measurement of Browser Versions in. *Group*. 2007

Furnell SM, Jusoh A, Katsabas D. (2005). The challenges of understanding and using security: A survey of end-users. *Computers & Security.* 5:27 - 35.

Griffith V., Jakobsson M. (2007). Messin' with Texas, Deriving Mother's Maiden Names Using Public Records. *RSA CryptoBytes*, 8(1), (2007), 18-28.

Hertzum M, Jørgensen N, Nørgaard M. (2004). Usable Security and E-Banking: Ease of Use vis-à-vis Security. 2004; 11.

Herzberg A, Jbara A. Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks. *Human Factors*. 2008;8(4):1-36.

Hutchinson D, Warren M. Security for Internet banking: a framework. *Logistics Information Management*. 2003;16(1):64-73.

Information gathering: http://www.bnm.gov.my/microsites/payment/04_paymentstats.htm

Jaspers MW. (2008). A comparison of usability methods for testing interactive health technologies: Methodological aspects and empirical evidence. *October*. 2008;8:340-353.

Jakobsson M., Myers S. (2007). Phishing and countermeasures: understanding the increasing problem of electronic identity theft, Wiley-Interscience, Hoboken, N.J., 2007

Just M.. (2005). Designing Authentication Systems with Challenge Questions in Designing Secure Systems that People Can Use. O'Reilly, L. Faith-Cranor, S. Garfinkel, editors.

Just M, Aspinall D. Personal Choice and Challenge Questions: A Security and Usability Assessment. *Security*. 2009.

Khalil M.N, Pearson J.M. (2007). The Influence of Trust on Internet Banking Acceptance. *Journal of Internet Banking and Commerce, August 2007,* vol. 12, no.2

Mannan M, Oorschot PC. (2007). Security and Usability: The Gap in Real-World Online Banking. *Human Factors*. 2007:1-14.

Mannan M, Oorschot PC. (2007). Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer. *Most*. 2007:88-103.

Mattila A and Mattila M. (2005). "How perceived security appears in the commercialisation of internet banking", International, *Journal of Financial Services Management,* vol. 1, no. 1, November, 2005, pp. 89-101.

Oorschot PC, Wan T. (2009). TwoStep: An Authentication Method. 2009 ;(3):233-239.

Vijayan, P., and Shanmugam, B. (2003). Service Quality Evaluation of Internet Banking In Malaysia. *Journal of Internet Banking and Commerce, 8 (1).*

Weir CS, Douglas G, Carruthers M, Jack M. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*. 2009;28(1-2):47-62. Available at: http://dx.doi.org/10.1016/j.cose.2008.09.008.

Wharton C, Je R, Fran A. Applying Cognitive Walkthrough Complex User Interfaces: To More Experiences, Issues, and Recommendations. *Computing*. 1992:381-388.

Wison S., "Digital signatures and the future of documentation", Information Management & Computer Security 7/2, 1999, pp. 83-87.

Yenyuen Y, Yeow PH. User Acceptance of Internet Banking Service in Malaysia. 2009:295-306.

Yiu C.S., Grant K., and Edgar D., Factors affecting the adoption of Internet Banking in Hong Kong-implications for the banking sector", *International Journal of Information Management,* vol. 27, October, 2007, pp. 336-351.

Zopolskia B.K., Kotulski Z. (2007). "Adaptable security mechanism for dynamic environments", Computers & Security, 2007, pp. 246–255.