Computer Security Issues in Online Banking: An Assessment from the Context of Usable Security

Computer Security Issues in Online Banking: An Assessment from the Context of Usable Security

FN Mahmadi, ZF Zaaba and A Osman

School of Computer Sciences, Universiti Sains Malaysia, Minden 11800 Penang, Malaysia

fnajmi.ucom12@student.usm.my, zarulfitri@usm.my, azam@usm.my

Abstract. Today's online banking is a convenient mode of finance management. Despite the ease of doing online banking, there are people that still sceptical in utilizing it due to perception and its security. This paper highlights the subject of online banking security in Malaysia, especially from the perspective of the end-users. The study is done by assessing human computer interaction, usability and security. An online survey utilising 137 participants was previously conducted to gain preliminary insights on security issues of online banking in Malaysia. Following from those results, 37 participants were interviewed to gauge deeper understanding about end-users perception on online banking within the context of usable security. The results suggested that most of the end-users are continuingly experiencing significant difficulties especially in relation to the technical terminologies, security features and other technical issues. Although the security features are provided to provide a shield or protection, users are still incapable to cope with the technical aspects of such implementation.

1. Introduction

The online banking provides the customer just about the whole services available in the conventional banking such as viewing accounts, making transactions, paying bills and handling finances [2]. Although the introduction of online banking brings big transformation between the bank - client speedy service interaction and service delivery, the aspects of online banking security still become the challenging issues. Previous studies also indicated that there are still significant levels of concerns over perception and trusting the system and its security [3, 4]. Operationally, online banking already provided security measures and preserved the confidentiality of online interaction to the end-user. Every time before an engagement is made online through the website, a process of identity authentication and verification is always a prerequisite before any further transaction is conducted. The authentication process is a process to validate or to verify the identity of the user as if the person is the valid user to the system [5]. During the authentication process, a piece of information is verified by the user utilising the username and password in order to gain access to activity or process. This piece of information also can be called as authentication factor which comes in various mechanisms of security devices such as smart card, token and security image.

A holistic understanding about the pros and cons of online banking, its risk and security, responsibility of parties involved (especially the bank, the client or even the online system provider if it is outsourced) should any breach of information, or even money lost happened, must be clearly understood before anyone is engaged in any form of online banking transaction. Clients in particular

must understand the calculated risk that they might facing and the protection available to them before they confidently opt-in for online banking in their transaction with the bank. [8].

This study is conducted to further investigate the usable security in Malaysia banking institutions from the views of end-users. The paper is organized as follows: Section 2 highlights the related work in relation to online banking in Malaysia which covers the aspects of usable security and possible risks, section 3 continues with the methodology that has been implemented, followed by the result and the discussion toward the interview process that has been done in Section 4. Finally in section 5 ending with conclusion and future works.

2. Related Study

End-users are not capable to protect themselves relying on the securely storing high-quality cryptographic keys as. Beyond that limitation, the designers have the responsibilities to design protocols that comply with its restriction [26]. Various security mechanisms have been developed in order to support the users in order to mitigate the consequences of vulnerabilities among the users. However, the security itself may jeopardize the users' decision toward their primary goal in the system as the users are the weakest link [27]. Thus comprehending the features is compulsory elements so that it can lead the end users with secure manner decisions.

The most important concern for every financial activity is to consider the environment of computer technology to be verified as safe and secure. Generally, a knowledgeable user is aware and concern about these aspects. However there are still users that only rely on their confidence level toward the technology they embraced, without knowing the possible risk that could jeopardize them. The identified risks are as the following; financial risks, security and privacy risks and usability risks.

2.1. Financial Risk

Financial risk to a customer is about loss of money or incidents that may response to inadequate finance that one supposes to have. Online banking transactions are not similar to conventional banking which provide formal meeting and tangible proceeding [12]. They are customers who are really concerned on losing their money when dealing with the online money transfer. In this case, end-users will be diffident to participate in any form of online banking services due to the risks and possible of loss especially when it involves a lot of money [13].

2.2. Security and Privacy Risks

When dealing with online banking, the possibility for the end-user to be exposed to the threat or attack by hackers is considerably high. A study showed that the end-user could lose the confidentiality of his/her critical information due to fraud or any unauthorized access of end-users record [9]. A similar study also indicated that the end users are also concerned about their personal data being corrupted due to virus, system crash and hacking [6]. These circumstances will in turn cause the end users to lose their confident in utilizing online banking.

Among methods that are familiar to online banking threats are phishing, pharming, man-in-the-middle attack, man-in-the-browser and malware attacks. Phishing, the activities of getting the user to give their personal information through fake websites, and pharming, the activity of modifying the DNS entries resulting users directed to the wrong website [15] are the two popular ways that hacker use to attempt on attacking users via Internet. Man-in-the-middle (MitM) attack is the type of attack use by hackers to listen to the communication between client and server by getting in between the sender and the recipient to access the traffic, modify it hence forward it back to the recipient as a threat [29]. One approach of attack is involving the pharming attack which compromises the DNS servers by the malicious code installed and redirect user to the fake website that can provide access to user credential and perform malicious activities [10]. Man-in-the-browser (MitB) on the other hand is a Trojan horse program which is a variant of the MitM attack. Man-in-browser attack is able to redirect the user to counterfeit site with the intention of attacking the user credential or information [16]. End-

users should be concerned on the malware attack as it will contaminate the host file and DNS as the attackers able to steal user credential and information. Based on highlighted instances, the security and privacy issues of online banking should be taken seriously. This is critical in order to come up with a more comprehensive and reliable security features that can assure end-users the comfort and confidence in online banking.

2.3. Usability Risks

Security in online banking is meant to make users feel secure and safe while login to the website. As such, the security features must be usable and not complicated in its steps because the technical terminologies could make users neglect from using the system instantly. Thus refrain from considering the security aspects that they have to consider [17]. A study has shown that technical terminologies become the common problems toward end-users to assist them in understanding the security features provided for them [18]. It is essential to create a system with high security but it should be consider on the factor whether it will be meaningful from the end-users perspective. Besides, the usability issues can be looked in term of the performance risk. Performance risk is a situation which occurs due to internal errors of the banking website. For example, server breakdown or Internet disconnections may happen which lead to the unpredictable loss [12]. Online banking help banks to reduce costs and speed up the delivery system. However, some factors must be considered such as the interfaces provided, type of services offered, delivery time and security features given. These factors may affect end-users' ability to adopt online banking. A study showed that online banking users are not satisfy with the delay services when transferring or receiving any payment which may be time consuming instead of fast, secure and convenient [13]. Incidences of technical and system hick-ups have become major problems in online banking services encountered by most of the end-users [14].

3. Methodology

We have conducted an online survey as a preliminary study in order to capture users' problems toward the issues of usable security in online banking websites. The online survey utilises 137 respondents which able to gain insights of the end-users difficulties and challenges while dealing with online banking (e.g. interfaces, terminology, and security). The results highlight the general perception of users in regards to security aspects in online banking. The majority claimed they facing significant problems in regards to technical terminology or jargon and explanation about technical aspects of warning and information. To further ascertain the results, an interview was used as the research tool to comprehend in depth of end-users' perception of usable security in online banking.

The purpose of the interview is to clarify further information or explanation that has been gathered in the online survey because this approach is considered to be able to increase the validity of similar studies conducted [17]. The choice of the interview also has been considered because it provided in-depth data collection which assessed in real-time discussion in order to examine the end-users' experiences and conceded various issues around online protection to be inspected [11].

The interview was conducted at the School of Computer Science, Universiti Sains Malaysia. The interview session was advertised within the campus via mailing list and word of mouth. This study utilized 37 participants of which 24 were male and 13 female. The participants involved were from the age of 18 years old and above and on voluntary participation. All participants are reminded that the dialogue will be recorded and will be used for research purpose. The participants are ensured that the information given by them will be treated as confidential as possible to maintain the integrity of the data. The participants were also reminded that they have right to withdraw at any stage of the session.

4. Result and Discussion

Table 1. Participants' information

Characteristic(n=37)		Frequency	Percentage
Gender	Male	24	65
	Female	13	35
Age	18-23	23	62
	24-30	14	38
Education	Postgraduate	36	97
Background	Undergraduate	1	3
Computer Skills	Beginner	7	19
	Intermediate	25	67.5
	Expert	5	13.5
Type of Participant	Technical	30	81
	Non-Technical	7	19

The demographic information from the participants from the interview were gathered and summarized as shown in Table 1. The participants were mainly male and ranging from the age of 18-23. All of the participants were undergraduate and postgraduate and had familiarity with computer and Internet usage. It can be indicated that having higher level of education may affect their thinking and decision making process. With regards to their skill in dealing with computer and Internet familiarity, most participants classified to be as intermediate level. Participants can be divided as technical and non-technical, Technical participants were derived from computer related background (e.g. Computer Science) while non-technical participants were derived from non-computer related study (e.g. Arts, Communication, etc.)

4.1. General Observation and Assessment

The first section of the interview was an overview of the participants with some general questions. The questions asked were basically about their experiences in dealing with online banking. The questions are as follows:

- Which online banking do you frequently used?
- On what purpose you usually do when doing online banking?
- Do you find any difficulties and problems while dealing with online banking?
- Do you find any informative guidelines, manual or help desk during your online banking? If yes, do you find it helpful for you and the end-users?
- Do you know all the features/function provided in the online banking?
- Do you know the security features equipped in your online banking website? Do you think it is sufficient?

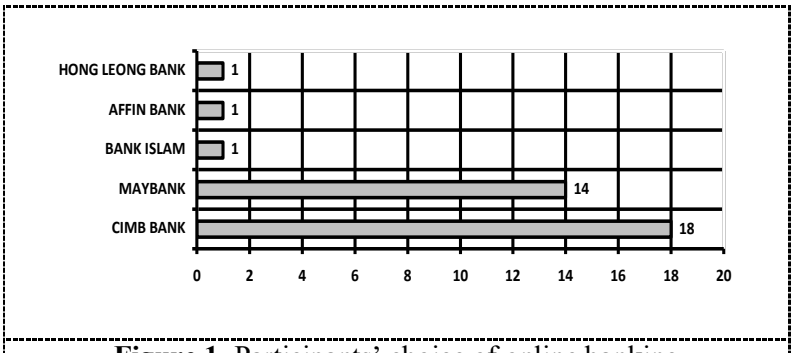

Figure 1. Participants' choice of online banking

Based on the responses given in the first section, the main choice for online banking services from 5 major banks in Malaysia were CIMB Bank and Maybank, whilst Bank Islam, Affin Bank and Hong Leong Bank was only being used by one participant respectively. Figure 1 illustrated the banking online services that the participants frequently used. From Figure 1 it had shown that only 35 participants involved because the remaining two participants interviewed are not using any online banking. Contributing factors on how the participants choose their preference is very much determined by the existing engagement that they already had with the bank. Other possible reason also due to the attractive interface and informative website that may attract the users (i.e. functionality, usability etc). On the other hand, end-users still experiencing challenges in online banking. The followings are some of the common difficulties encountered based on feedbacks quoted from the participants as shown in Table 2.

Table 2. Responses regarding the problems and difficulties when dealing with online banking website

Responses regarding the problems and difficulties when dealing with online banking website
Participants 5- "*Actually at first I need to analyze first the function on online banking and then after I familiarize all the function and then I just proceed to my stuff.*"
Participants 8- "*Yes. A bit about the security. I'm not sure if my online banking website is secure enough."*
Participants 13- "*Sometimes, certain bank got the problems with the interface which is too complex and sometimes too simple and not interesting to be logged into."*
Participant 19- "*I think the online banking website is not secure enough."*
Participants 23- "*Yes. The interfaces is too complex and they are no manuals to help the users."*
Participants 28- "*For me I think I have the problems with the interfaces provided there. Sometimes when I need to do something like to check for history of transaction it has consume me a long times."*

Several participants acknowledge that they do sometimes face different nature of problems with the banking website. These problems can be the interfaces, security features, general functionalities and others. There are instances where the complicated online banking system failed to benefit them due to the complexity of the steps and interfaces which in the end caused them to quit. Other contributing factor is unavailability of guidance to complete tasks that end-up the user with self-familiarization by means of trial and error which is time consuming and daunting tasks for first timers. Apart from that, there are few participants, which stated that they feel unsure about the security provided for them in online banking website which affects their behavior and assessment towards online banking.

When they were asked on the security features readily available in the online banking websites, the author only managed to capture 6 participants that realized the presence of "https" instead of "http" in the address bar of the banking. When they were asked, they do realized the functionalities which is to ensure the security of their banking website. They do realize the importance of this feature so that they will not get tricked into fake website and give their information to the hackers easily. Although the answers generally encouraging but Figure 2 on the other hand reflected different connotation on how users perceive satisfaction towards security features. It can be noted that most of the users were not satisfied with the current security provided while a few were not sure about their feeling. Most of the participants opined that some adjustment or improvement should be made to the banking website in order to create the sense of security for its end-user when doing transaction through online banking which can ensure the feeling of secure while dealing with online banking. Additional layers for authenticity check can be created (as an example) to address this concern as suggested by some of the respondents.

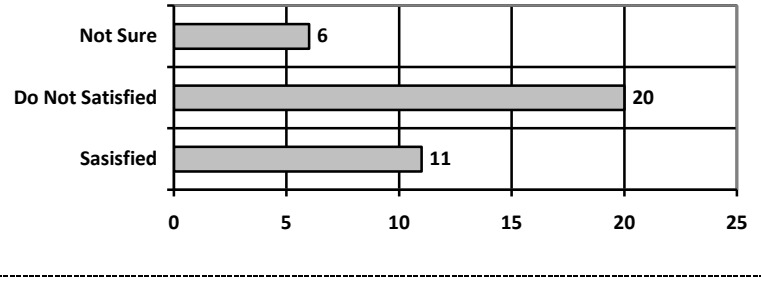

Figure 2. Satisfaction toward current security features

5. Scenario-based Questions and Discussion

A scenario based questions were asked with two scenarios as shown in Figure 3 and Figure 4. No information or hint is given about the scenarios presented to them as the purpose is to assess and examine the participants thought and understanding. The interview continued with several questions for each scenario that has been presented to the participants. The questions are as the following:

- Do you know what this is?
- Do you know how to derive this?
- Do you understand what it means?
- What difficulties do you encounter when accessing information from this? Any other?

Figure 3. Scenario 1[23]

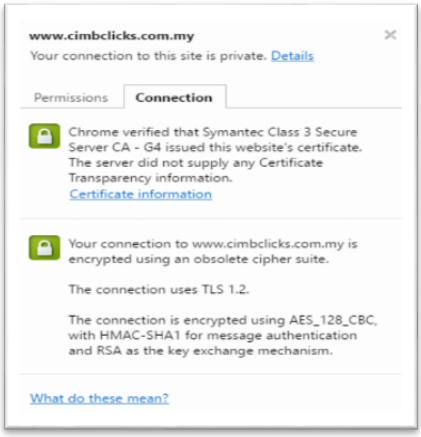

Figure 4. Scenario 2[23]

Through Scenario 1, the participants realized that it was a website address from one of the Malaysian banking website login page. The participants were asked to give their thoughts based on scenario 1 shown to them. Some of participants were able to notify some of the security features available such as the present of https, the lock icon and the green color on the website address bar. However, there a few of them who were less observant and unable to explain the usage of these features. Figure 5 indicate the responses between two contradictions regarding the presentation of https, the lock icon and the green color. It can be revealed that most of the participants realized the presentation of the features mentioned earlier in the scenario presented to them. However, there are still a number of participants did not realize the security features at all. There were two reasons for this

outcome where respondents that had technical background were mostly observant of these security features and were able to explain them technically, whereas the non-technical background respondents unable to do that. Thus, it can be noted that non-technical generally were not familiar with the most of the security features provided for them.

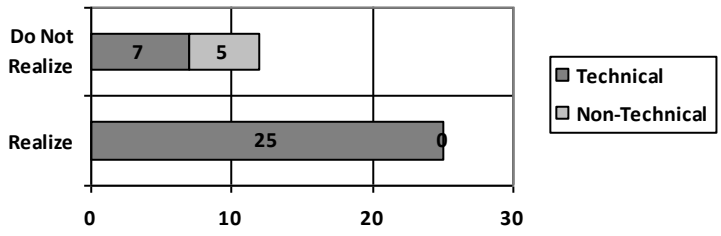

Figure 5. Participants' response regarding the presentation of https, the lock icon and the green color.

The second scenario as shown in Figure 4 is about the digital certificate available in the online banking website. Digital certificate is a security certificate that use as a form of certification protocol to certify the people, the website and the network resources from a reliable source. It also provide protection for data exchange from the visitor and the website from being tampered or even from identity theft [22]. The digital certificate in the context of banking website plays a role of securing data exchange within the system [21]. Hence, the end-users should take it as important feature in security when dealing with virtual finance activity in order to prevent any intrusion or identity theft from potentially happening.

The participants were asked whether they understand the purpose of the digital certificates. The results revealed that only 4 participants understood the purpose and the remaining 33 participants were still in baffled. It should be noted that the result of participants stating they know the feature as digital certificate is 7 participants opposed with 30 participants whose cannot identify the feature as digital certificate. There is an increase on number of participants stating that they do not understand the feature even though they stated that they do know what the feature is. Given said this, it can be depicted that although the end-users do know the security provided for them, it cannot be assured that not every end-users able to understand the purpose of it and apply it for their own use. Based on the result, it can be depicted that the knowledge of this feature also comprehend majority of technical users too instead of only non-technical users that was expected in this experiment. The result was taken from the same number of participants when asked on whether they know how to derive the feature. It can be assumed that majority of the participants do not know how to derive the feature because they never come across it before. For instance, participant no.33 identified as technical user was asked whether he/she knew the Scenario 2 presented to them.

Participant no.33 was able to identify the feature as digital certificate but unable to explain further regarding its purposes. Assessing the cause of it, the participant no.33 claimed that the feature was mentioned as digital certificate but he/she unsure about the main functionalities. It is shown that the end-user may know something from the surface rather than in depth knowledge about the features.

Participant 33 "I only know its name and how to get it. I don't know the actual function of it."

To gain more information regarding the participants' perception, they were asked to explain the problems they faced when accessing the information from these kind of scenario. Table 3 indicates the feedbacks given by some of the participants involved in the interview regarding this matter. Based on the feedback most of them were having almost similar difficulties to comprehend the digital

certificate. Having said that, the information provided were rather too technical for laymen. The jargons used such as "digital signature", "verify" and "authentication" are not suitable for end-users especially for the non-technical background. In fact, such difficulties even faced by the participants with technical background too. This has been a common issue when talking about security features based on online transaction. Many prior research works have highlighted the same issues beforehand [12, 17, 19]. Preferably it is good to have a very reliable security protocol in any online transaction especially banking, but if the end-user fail to appreciate and take the advantage of the given protection, obviously the security aspect of it will easily be compromised.

Table 3. Problems or difficulties faced by participants

Responses
Participant 1-*"Maybe the use of terms like verisign Class, international server. As for us computer science student we might understand what it means. But for the other people may did not know what it means."*
Participant 28-"*I hardly understand the meaning of certain words in there and what it actual trying to describe. I don't bother to search for it because it will be troublesome and may take some times. For me I find it difficult to understand even though I am computer science student. I guess it is for security reason but there should be some explanation provided. For non-technical person, it would be difficult and confusing, if not totally unaware about this security features at all."*
Participant 35- *"The technical terms are quite hard for me to explain. They need to elaborate more for ease of end-users."*
Participant 37- *"Definitely it is difficult to understand all of this. The terminologies and words here is hard to be explained especially for the common users."*

An interesting finding as shown in Table 4 indicated that, one's perception and understanding on the security features involved in any form of online transaction is very much related to his/her level of skills or knowledge in computer technology. For instance, a person who is an IT savvy would have a different point of opinion and experience about this subject matter as compared to one who is not [1, 11]. Having said that, it show significant needs to develop a website equipped with features and functions that are user friendly to its end-users, especially those with non-technical background. Only then, the trend in using online transaction would be more convincing among the potential customers.

Table 4. Intermediate and expert user statements

Responses
Participant 11- "*I think the main problem for me is that I don't really know that this feature exist and what it is all about. I think the common people may also be confused with it and what purpose it is for."*- intermediate user
Participant 24- *"I can understand almost 75% of the functions words here. Being a computer science student, it is easier for me but I don't think the common users without the technical knowledge will understand all of this easily."* –expert user

Referring back the objectives, the study is conducted to further investigate the usable security in Malaysia banking institutions from the perspective of the end-users. The preliminary results from 137 participants confirm that online banking in Malaysia still facing significant problems and issues. From the results of the interviews, it can be confirmed that majority of them continuously facing difficulties while dealing with online banking (e.g. interfaces, help and services, security, etc.) The choice of selecting the two scenarios (i.e. online banking URL and digital certificate) in the interview was due to the familiarity of the de facto Internet banking standard which is being used by all banking website in the world to clarify the confidentiality and integrity based on the Secure Socket Layer/ Transport Socket Layer scheme [28]. Although the scenarios might look straight forward, it can be the basis to

understand the foundation layers of users' comprehension in regards to online banking. An online survey finding indicates that more than 70% of respondents stated that they did not understand the digital certificate shown to them and 95% of them suggested that the Malaysian online banking need to be improved. The interview results also reaffirm the results and revealed that the majority of participants were not fully understood the concept and the security provided for them while performing online banking (i.e. digital certificate, https, contents of digital certificate etc) as mentioned in previous discussion.

Security is meant to be designed for end-users [26]. As the core purpose is to help the end-users, it should be meaningful and usable in a way the user manage to benefit from it. By stating the term usable, the security must be designed to be well understood and easy to be used by the end-users. The results of the interview also manage to highlight that the majority of the participants which were unable to derive the digital certificate from the online banking websites (i.e. unable to show how to derive the full version of digital certificate). By this, it can be noted that the digital certificate which act as one of the core of security in the online banking websites cannot be identified as effective for the end-users. The security of the systems can be said as effective if the end-users can used the security tools provided correctly [25]. End-users should be capable to understand the system and security so that they might avoid unnecessary errors while performing online banking.

6. Conclusion

Advancement in technology has transformed a lot of work processes into becoming easier, faster and reachable from your home without having the hassle to queue in getting most of the services that you need. Thus, in leveraging its customer services, most banks facilitate the online banking in all of its products to their intended customers. On the contrary, advancement in technology is not crime-free too. Acknowledging with many possible menaces, every banking institution have provided some means of protection to its client in order to ensure the customers that their online transaction with the bank is secure. For that reason, most banks have equipped many security features such as SSL and digital certificate as protection not only for them but their customers too. The results from the interview revealed the similar outcomes where end-users unable to comprehend the technical terminology and the meaning of those features. Having security features are good as precaution. The developer should find the best way to provide clear explanation so that it can accommodate any types of users. Having 37 participants might be a small sample. However, it gives useful facts that can be gathered for the developer or any practitioners' to reconsider presenting those technical functions.
Whether all these security features are being acceptable and utilize to the fullest by the end-users, are still debatable. This is true because efforts to increase the level of awareness among end-users need to be taken seriously. Therefore better understanding on this subject would give the sense of trust and security for the end-users to engage in secure manner in online transactions.

References

[1] Furnell, S. M., Jusoh, A., Katsabas, D. and Dowland, P. S. (2006b) 'Considering the Usability of End-User Security Software', *Proceedings of 21st IFIP International Information Security Conference (IFIP SEC 2006).* Karlstad, Sweden. Springer Boston, pp. 307-316.

[2] Major Capabilities of Online Banking. [Online] Available at: http://wps.prenhall.com/wps/media/objects/2519/2580469/addit_chmatl/TURBMC03_0131854615Ex.pdf (Accessed: 20th September 2015)

[3] Aladwani, A.M (2001). "Online banking: a field study of drivers, development challenges, and expectations". International Journal of Information Management. Vol 21, pp. 213-225.

[4] Suh, B., Han, I. (2002). "Effect of trust on customer acceptance of Internet banking. Electronic Commerce Research and Application". Vol 1. pp. 247-26

[5] Liou J. C., Bhashyam S. "A Feasible and Cost Effective Two-Factor Authentication for Online Transaction" *Software Engineering and Data Mining (SEDM), 2010 2nd International Conference* on. pp. 47-51

[6] Jassal R. K., Sehgal R. K. (2013). "Online Banking Security Flaws: A Study". *International Journal of Advanced Research in Computer Science and Software Engineering*. Vol 3. Issue 8. pp. 1016-1021
[7] US-CERT (2008). "Banking Securely Online" [Online] Available at: https://www.us-cert.gov/sites/default/files/publications/Banking_Securely_Online07102006.pdf (Accessed on: 20th September 2015)
[8] Karim Z., Rezaul K.M., Hossain A., (2009) "Towards secure information systems in online banking in Internet Technology and Secured Transactions". *ICITST 2009. International Conference* , vol., no., pp.1-6, 9-12
[9] David C. Chou, Amy Y. Chou. (2000) "A Guide to Internet Revolution in Banking, the E-Commerce Revolution". *Information System Management*. Vol 17. pp. 1-7
[10] Whitten A., & Tygar, J. D. (1999). "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." *Usenix Security* Vol. 1999.
[11] Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security*, Vol 27. Issue 7. pp. 235-240.
[12] Kuisma, T., Laukkanen, T., and Hiltunen, M. (2007). Mapping the reasons for resistance to internet banking: a means-end approach. *International Journal of Information Management,* 27(2), 75–85.
[13] Lee, M. C. (2008). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, 8, 130–141.
[14] Agarwal, R., Rastogi, S. & Mehrotra, A. (2009). Customers' perspectives regarding e-banking in an emerging economy. *Journal of Retailing and Consumer Services,* 16, 340-351.
[15] Karapanos N., Capkun S. "On the Effective Prevention of TLS Man-In-The-Middle Attacks in Web Applications". *USENIX Security Symposium*. USENIX Association. Vol 23. pp. 671-686
[16] Cain C. (2014). ' Analysing on man in the browser attack" *SANS Intitute InfoSec Reading Room* pp.1-23
[17] Bravo-Lillo, C., Cranor, L. F., Downs, J. S. and Komanduri, S. (2011b) 'Bridging the Gap in Computer Security Warnings: A Mental Model Approach', Security & Privacy, *IEEE,* vol.9, 2, pp. 18-26.
[18] Nowack, M. (1997), 'The Impact of the Internet on Statistical Organisations', *Statistical Journal of the UN Economic Commission for Europe,* vol.14, 4, pp. 345-355.
[19] Zaaba Z. F, Furnell, S.M, & Dowland, PS, (2011). 'End-User Perceptions and Usability of Information Security', *Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA). London*, UK, pp. 97-107.
[20] Raja, F, Hawkey, K, Hsu, S, Wang, KLC, & Beznosov, K (2011).'A brick wall, a locked door, and a bandit: A physical security metaphor for firewall warnings', *Proceedings of the Seventh Symposium on Usable Privacy and Security.* Pittsburgh, USA, pp. 1-20.
[21] O'Brien, M., & Weir, G. R. (2008). "Understanding digital certificates." *Proceedings of the 2nd International Conference on Cybercrime Forensics Education & Training.*
[22] Al-Khouri, A. M. (2012). PKI in government digital identity management systems. *European Journal of ePractice*, 4, 4
[23] CIMB Bank Berhad (2016). "CIMB Clicks" [Online] Available at: https://www.cimbclicks.com.my/ibk/ (Accessed: 5th May 2016)
[24] Wiersma, W. (2013). The validity of surveys: Online and offline. [Online] Available at: http://papers.wybowiersma.net/abstracts/Wiersma,Wybo,The_validity_of_surveys_online_and_offline.pdf (Accessed: 5th May 2016)
[25] Sasse, M.A, Flechais, I. (2005). "Security: Why Do We Need It? How Do We Get It?" Cranor, LF and Garfinkel, S, (eds.) S*ecurity and Usability: Designing secure systems that people can use.* pp. 13 - 30 ISBN: 9780596008277

[26] Kaufman C., Perlman R., and Speciner M. (2002) "Network Security: PRIVATE Communication in a PUBLIC World". 2nd edition Prentice Hall, pp. 237
[27] Whitten A., and Tygar, J. D. (1999). "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." Usenix Security Vol. 1999.
[28] Katsabas D., Furnell S. M., Phippen A. D. (2004). IT Security: A Human Computer Interaction Perspective. *Advances in Network and Communications Engineering* 2, pp. 35.
[29] Eriksson, M. (2003). An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions, *International Conference on Applied Cryptography and Network Security.*