Journal of Engineering and Applied Sciences 13 (3): 709-716, 2018
ISSN: 1816-949X

Preliminary Study on Security Issues of Online Banking: A Case Study of Malaysia

Faiz Najmi Mahmadi and Zarul Fitri Zaaba
School of Computer Sciences, University Sains Malaysia, Minden, 11800 Penang, Malaysia

Abstract: The banking institutions introduce the facility to do online banking whereby people able to manage their finances at the tip of their finger anytime and anywhere with the present of internet. However, there are significant issues that need to be look upon such as the security and privacy challenges, security implementation and users awareness. This research highlights the preliminary study on security issues in online banking in Malaysia utilizing a survey study with 136 respondents. The results suggested that end-users are still experience significant problems in relation to security and usability issues. The end-users perceptions are gathered to provide a basis to improve the current implementation of online banking website in Malaysia.

Key words: Usability, usable security, security, privacy, online banking, information system

INTRODUCTION

Since, technology evolves, the banking institutions system need to comply with that fast evolution. In the virtual era where internet is widely used, online banking has made almost everything possible. An online banking (i.e., also known as internet banking or web banking) is the usual or normal banking transaction activities utilizing the internet (Investopedia, 2015). The online banking will provide the customer with similar services available in conventional way such as view accounts, make transactions, pay bills, handle finances, etc. (Investopedia, 2015).

As the online banking is widely used, there are issues highlighted which are related to perceive of trust, security and privacy (Aladwani, 2001; Suh and Han, 2002). The online banking secures the confidential of access to website utilizing the authentication process. The authentication process is a process which is to validate or verify the identity of the user as if the person is the valid user to the system (Liou and Bhashyam, 2010). During the authentication process, a piece of information is verified by the user like the username and password to gain access to activity or process. This piece of information also known as authentication factor which comes in various mechanisms such as the use security devices of smart card or token, security image, etc.

On the other hand, the aspects of security awareness of the online banking are also crucial amongst the end-users and developers. The online banking platform must be integrated to satisfy the end-users need without compromising any security risks that might be occurred. The developers need to provide the best security defense to secure the online banking and at the same time it is understandable or usable to the end-users. One challenge that might occur from the perspective of developers is to elucidate the technical information or the process involve in the online banking.

Some questions that might pondering in the users mind when they assessing the online banking website; Do they understand the risks available on every transaction in their bank website? Do they know the security features available for them to facilitate the secure transaction? Do they feel confident about the security implementation in their bank website? For every security breach or incident occurs, the responsibility must come hand in hand amongst the end-users and the online banking provider (i.e., actors in the trust of chain). Thus, as the end-users, they should aware of this situation and should not only rely to the system provided but take the proactive solution to understand the whole security system and the potential risks they might facing with. The outline of this paper is as follows: background study highlights research that had been conducted within the security issues; guideline and overall view section discuss the need of security compliance for online banking; results and discussion section explains the analysis of the results based on the survey study and finally, ending with conclusion and future researchers which explain the importance of this study and expected works to be done.

Corresponding Author: Zarul Fitri Zaaba, School of Computer Sciences, University Sains Malaysia, Minden, 11800 Penang, Malaysia

Literature review

Background study: Internet has become a vital role which has morphed into a way how people live their life. Since, the rise of the internet, the online banking is made possible in the circa of 1980's (Canstar, 2013).

In 1970's, an activity called home banking has been introduced which involve financial institutions do business via. touch-tone telephone. Later, the usage of cable television approach has brought up an advantage to solve the graphic limitations of the touch-tone telephone. However, somehow it has the absence of two-way communication. As the PC era arrived, the visual display and two-way communication is made possible. This so called PC has been considered as an ideal device for online banking. With the development of technology nowadays, online banking has been used on various devices such as PDA, mobile devices and etc. The online banking service can be implemented through the four media which are online banking using the bank's proprietary software, online banking via. Pc using dial-up software, online banking via online services and internet banking via. web (Chou, 2000).

Nowadays, Central Bank of Malaysia (Bank Negara Malaysia) has approved the license total of 59 banking institutions in Malaysia not only the institutions from the local level but also the Foreign institutions (BNM., 2015). On the other hand, the financial institutions licensed in Malaysia are categorized in 5 categories which are commercial banks, Islamic banks, international Islamic banks, investment banks and other financial institutions. There are a total of 27 financial institutions licensed as commercial banks and the Islamic banks are counted to be 19. As for the investment banks and other financial institutions both are count to be 11 and 2 in numbers.

As the financial institutions are growing in Malaysia, each institution keeps competing in their own way giving the best services. With the presence of the internet, financial activities have been made available and possible in many ways. Therefore each banking institutions will have their own way to publicize their services and online transactions (i.e., via. online banking website). The next section will discuss further on the challenges in online banking.

Security and privacy challenges in online banking: Some people may state that privacy can always be universally associated with the term "security" as the similar. However, this fact is not true. Security is the protection against the condition or event with the potential to cause economic hardship to data or network resources in form of destruction, disclosure, modification of data, denial of service, fraud, waste and abuse (Belanger *et al*., 2002). On the other hand, (Warren and Brandeis, 1890) define the privacy as a legal concept and as the right to be alone. Internet privacy is mostly information privacy which means the ability of the individual to control information about one's self (Yang, 2015).

Online banking is facing various challenges in relation to security and privacy (Yang, 2015; Kelly and Kenzie, 2002). With the recent technologies, hackers are growing rapidly and targeting the unsecured bank website where later on it will compromise the security for users (Jassal and Sehgal, 2013). From day to day basis, the attack may evolve to a different level as indicate in Fig. 1 (Easy Solution Inc., 2015).

From Gartner in his report (April 2, 2009), "The War on Phishing is Far From Over", states that 5 million consumer of the United State of America population

Fig. 1: Evolution of threat (Easy Solution Inc., 2015)

already lost money due to phishing attack and its variants through the end of September. Malaysian Computer Emergency Response Team abbreviated as MyCERT claimed in their report that the phishing scams are rising in numbers in Malaysia more than the hacking threats involving four local banks has been victims during 2005 (BolehVPN, 2013). The incident of intrusion attempt, denial service, cyber harassment and malicious codes have decreased in number while fraud and scam, vulnerability report, content related and intrusion have increased in number through the 2nd quarter of 2011. These incidents indicate many possible menaces occurs which beyond our control on day to day basis.

Guideline for security in online banking: To ensure the security in online banking, various mechanisms have been used in the online banking financial institutions. It should be periodically follows this term along to be consistent with the guideline providedproduced by the FFIEC Information Technology Examination Handbook, Information Security Booklet, December 2002 (FFIB., 2011):

- To ensure their information security program to identify and assess the risks associated with internet based products and services and to identify risk mitigation actions, including appropriate authentication strength and measures and evaluates customer awareness efforts
- Adjust as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information and internal or external threats to information
- Appropriate risk mitigation strategies should be implemented

Authentication mechanisms: In general authentication is a process of determining for someone or something, who or what is identified and verified to be (IU., 2014; BU., 2015). In online banking, the authentication is a security process as the identification factor to keep someone information to be secured to access their financial activities (Thigpen, 2015). There are three authentication methodologies to be found which focusing on three basic factors depending on the term 'knows', 'has' and 'is' (FFIB., 2011). Something the user know means the most common factor used such as password or PIN. Something the user has refer to the item user possess such as smart card and hand-held token while something the user is refer to the user itself which highlights the usage biometrics.

MATERIALS AND METHODS

Something the users know

Username and password: This is the most basic form of security mechanisms. This authentication method required the user to create a unique username as identifier and to provide the secret passwords to enable them proceed to the system. Most of the current systems are using the authentication methods as their basic security mechanisms. However, the threats of targeting passwords have become easier to implement with the rises of the technology implementation and development.

In addition passwords are highly susceptible to be exposed to the man in the middle attacks (Katz, 2002; Thigpen, 2015) and also to someone who watches you enter the code. Even a secure password which been made difficult to be remembered to the users, a phishing and spoofing attacks may attack the users by creating a similar look/ legitimate website to trick the users to applying the password (Liou and Bhashyam, 2010).

PIN is the short form of "Personal identification number". The most common use of PIN is in the Automated Teller Machines (ATM). This authentication method also exposed to the threats similar to the used of username and password (Katz, 2002; Thigpen, 2015). Albeit the 8 pin digits used with the current technology, the encrypted pin can be decrypted within few seconds.

Identifiable picture: Identifiable picture is one of the latest security mechanisms applied to the online banking website. Some banks in Malaysia are beginning to integrate pictures as part of their authentication systems. These type of authentication act as an extra layer of the authentication in order to assure that the user is at valid online banking site by verifying the picture first to enter the legal site (Madhuravani and Reddy, 2013). This picture also can be said as a generator factor to a graphical password (Prasad and Kuma, 2015).

One time password: One time password is the authentication which similar to username and password but somehow difference as the password never entering the public network. One method for accomplishing a one-time password authentication is require the system uses a client side generator and a server. The user will provide a secret password to the generator to be accepted and then it will be concatenated with information sent from the server in control of authentication (Thigpen, 2015). The advantage of this type of authentication is it can protect the user against the passive attacks which may be vulnerable on normal password.

Something the user has

Swipe card: One of the examples of the swipe cards is the credit card. This type of authentication can be used in conjunction with other authentication mechanisms like PIN. These cards are small and contain a magnetic strip which has a function to hold the user's identity information. The card itself also possesses the risk of theft as the data held by the card can be duplicated by means of proper equipment (Thigpen, 2015).

Proximity card: The way of proximity card work is identical as the swipe card but somehow it work from a distance from vender to vender. This card has the information to authenticate the user possess the card as the person who is verified to gain access to the resources. The card reader reads the information when the card is placed to the card reader and the information is exchanged wirelessly. The proximity card however shares similar problems with the swipe card (Thigpen, 2015).

Smart card: Smart card is the successor of the magnetic card that is widely used in credit cards, debit cards, ATM cards and ID badges (Liou and Bhashyam, 2010). Smart card size is about the same size like other magnetic cards but somehow require a special reader. It also requires special middleware applications (i.e., smartcard communication standards and the communication protocols used by the mainstream PC application is mismatch).

USB token: USB token has to be plugged into a computer's USB port to be used. This token contains the information of the holder's identity and act as a method for the holder to gain access to his/her resources. Usually, these token has been installed withsoftware licensing information which make the holder feel secured to monitor their financial record. However, the risk of the token to be stolen or broken should be considered as the flaw of USB token.

Something the user is

Biometric: Any automatically measurable, robust and distinctive physical characteristic that can be used to verify or validate the identity of an individual is referred as biometrics. Since, each people has unique physical properties which are based on their heredity, biometric characteristic are difficult to be tampered (Liou and Bhashyam, 2010; Thigpen, 2015). For many biometric identifiers, the actual biometric information is rendered into string or mathematic information. Using special provided hardware, users may authenticate via fingerprint, voiceprint, hand geometry and even iris scan. After the user is authenticated as the verified user, the user will be directed to the PIN or password authentication (Liou and Bhashyam, 2010). However, when a large number of users are authenticated at the same time, this method will be inefficient and comparatively expensive (Liou and Bhashyam, 2010).

Fig. 2: Security information guidance (CimbClicks, 2015)

Digital certificate: Digital certificate acts like an electronic passport or an electronic identification which allows the person, computer or organizations to exchange information securely via. internet using the Public Key Infrastructure (PKI) (Preeti, 2014). A certificate is digitally signed by a root certificate which is belonging to a trusted Certificate Authority (CA). Website protected by certificate displays a lock icon as followed by the "https" on the leftmost part of the URL's site. In order to view the certificate content, user needs to click on the lock icon and more details information will be provided. However, the explanation about it is using technical terminology rather than laymen term.

Security information guidance: Security information guidance is security information presented to the users every time they assess the online banking website. The purpose of this feature is to encourage the user to take a precaution about the possible menaces and to advise them on what to do to minimize the risks level. This feature usually come in the form of advertisement pop up window when log into the website or either to be put in a section where seem to be reliable to be seen by the user. Most of the banking institutions use this medium to share with their customer about the safety guidance as shown in Fig. 2.

The most important concern for every financial activity is to consider the environment of computer technology to be verified as safe and secure. Malaysian banking websites have adapted various types of mechanisms in aforementioned section 2.2 to ensure the security of the website. Although, the banks provided their online banking with variety of ways of security protection, users should also take their responsibility in terms of self-awareness toward this incident.

In fact, BolehVPN (2013) highlighted a surprise results when testedone of Malaysian banking website that having among the highest customers where the results indicated with Grade F regarding the support to SSL 2.0 and weak Cipher. Thus, it can be suggested as how complex and dynamic the equation involve in providing security for online banking. The developer need to balance on the ease of use and the important of security (i.e., without jeopardizing the confidentiality, integrity and availability), so that, users from different background able to use it in secure manner.

RESULTS AND DISCUSSION

In aforementioned study, an overall view highlighted the perspective of security in online banking in Malaysia. This study discusses the survey study to gain general insights on how general public understand the perspective of online banking in Malaysia in regards to security. The survey was well promoted in the university environment. This survey gathered a total of 136 respondents where the majorities are comprised of the users from the age group of 18-25 and the outcomeis not to be surprised as this age of group is the majority of the internet users in Malaysia. These survey consist of 3 parts of questions. On the first part, the respondents were asked on whether they are performing any online banking. For those saying yes, they were guided into part 2 and 3 of the survey while the others proceeded to part 3 questions. Table 1 indicates the summary/results of the online survey.

Respondents were asked whether they performed any online banking and 75.7% of the respondents claimed to useonline banking. Majority of the respondent's stated that they feel secured and rated the security implementation in the online banking website as god security. However, almost 40% were still not sure about it.

Next, a pop up advertisement of one Malaysian banking website has been shown to them in the form of image and asked whether they read it once they receive it. Figure 3 portrayed the example of the pop up advertisement. Majority of the respondents experienced this advertisement and they tend to ignore and close the pop up advertisement without read it first even though the information were well provided for them. Most of them also stated that this feature always upset them (i.e., repeating). Next a digital certificate is shown to the respondents as depicted in Fig. 3 and 4. From the results, 65% of them stated that they did not realize about these feature. Most of them were also not aware and not comprehended about this feature at all. Having said that, the information provided were rather too technical for laymen. The jargon usage for instance "digital signature", "verify", "authentication" and etc were not suitable for non-computer background.

In the last section, the respondents were asked on three types of questions. The respondents were asked to rate the security implementation in online banking Malaysia.

Table 1: Summary of online survey

Characteristic (n = 136)	Count	Percentage
Part 1: To every respondent (n = 136)		
Do you use online banking?		
Yes	103	75.7
No	33	24.3
Part 2: Online banking user (n = 103)		
Do you feel secure when you do online banking?		
Yes	69	67
No	7	6.8
Not sure	27	26.2
How would you rate the security implementation in you online banking website?		
1. Less secure	0	0
2.	4	3.9
3.	37	35.9
4.	56	54.4
5. High security	6	5.8
Below is a pop up advertisement of one of Malaysian banking website. What did you do when you encounter the pop up advertisement?		
Read it before close it	42	40.8
Close it before read it	61	59.2
Below is the feature available in secure connection. Do you know about this feature? (An image of digital certificate is shown)		
Yes	36	35
No	67	65
Do you aware the importance of this feature?		
Yes	43	41.7
No	60	58.3
Do you understand about this feature?		
Yes	33	32
No	70	68
Part 3: TO Every respondant (n = 136)		
How do you rate the security implementation in Malaysian banking website?		
1. Less secure	1	0.7
2.	9	6.7
3. Unsure	72	53.3
4.	49	36.3
5. High security	4	3
Do you think Malaysian banking website still need improvement?		
Yes	129	94.9
No	7	5.1

Fig. 3: Pop up advertisement (Maybank2u, 2015)

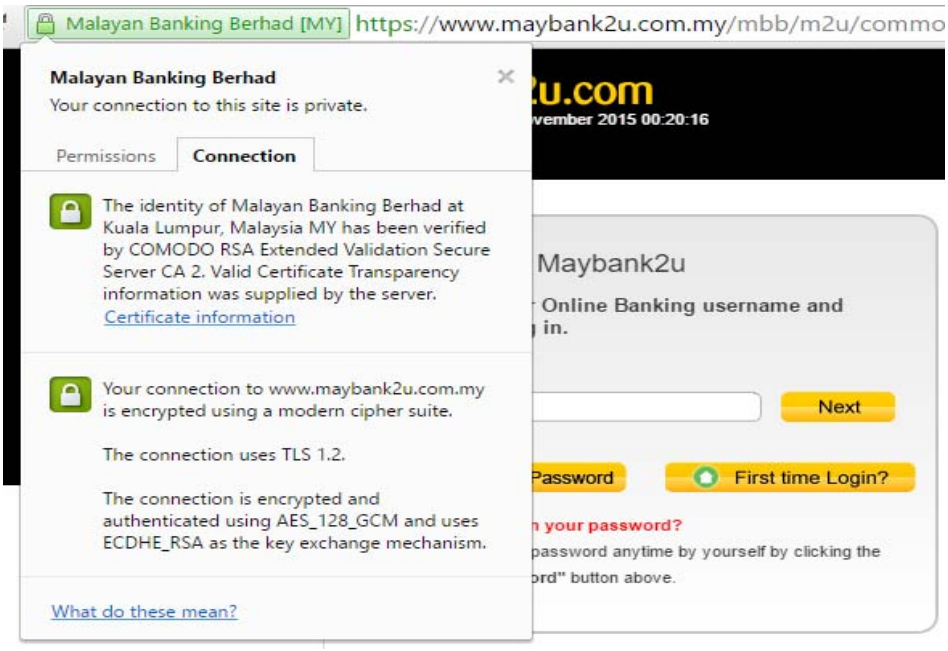

Fig. 4: Digital certificate (Steven, 2005)

In part 2, there were 103 respondents answered the questions (i.e., those who experienced using online banking) while in part 3, all respondents answered the question. A surprising finding can be highlighted within this section as shown in Fig. 5 where similar question has been asked in part 2 and 3, respectively. Initially, 54% claimed the online banking website is secured and 36% unsure (i.e., those who experienced with online banking). On the other hand, we asked again similar question to all participants and results indicated 36% claimed the website is secured and the unsure percentage increased to 53%.

It can be noted after respondents experienced series of questions in relation to the security of online banking,

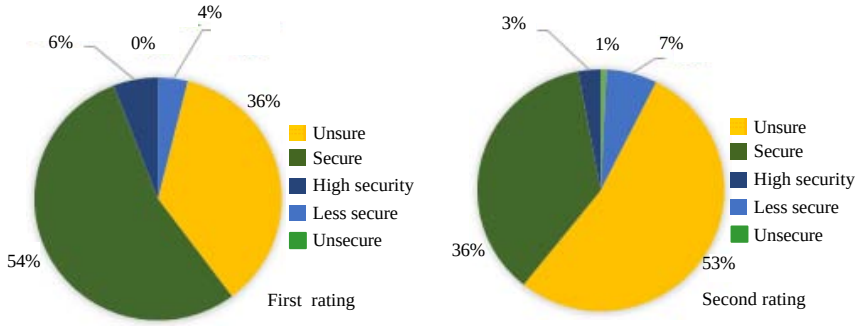

Fig. 5: Rating of security

they started to realize the real problems existed facing by the others (i.e., after viewed the image, knowing the incidents, etc.) and thus they might changed their perception accordingly. In addition, the results suggested that current online banking website still need to be improved as claimed by 94.9% of respondents. Having said that, end-users came from different background and it was significantly affects their decision making process and their understanding. Thus, this survey manages to highlight preliminary insightsand suggests that there is a corresponding need to improve the online banking website in terms of usability (i.e., usable security) (Zaaba *et al*., 2014; Zaaba and Boon, 2015).

CONCLUSION

Banking institutions in Malaysia has advancing their service to enable their customers in virtualization of banking features called online banking. With the development of this feature to this service, customers as users are rising to add this service to their financial activity. However, there are still significant issues and challenges that need to be taken care of. The presentation of the online banking website is varies from one and another.

It is good to provide the highest security approaches to secure the transaction however it is not meaningful if end-users unable to appreciate the features and the protection provided for them. Therefore, it is important to understand the security perception of end-users, so that, the website can be created in secure manner and more meaningful (i.e., usable security). For future works, an interview session will be conducted to get further understanding on what specific elements need to be enhanced or improve. Gathering these evidences will provide a foundation to develop a better and secure online banking website to the developers and research community.

ACKNOWLEDGEMENT

I am grateful to complete this study with the help of my supervisor Dr. Zarul Fitri Zaaba. This is the preliminary study of my final year research project.

REFERENCES

Aladwani, A.M., 2001. Online banking: A field study of drivers development challenges and expectations. Int. J. Inf. Manage., 21: 213-225.

BNM., 2015. List of licensed banking institution in Malaysia. Bank Negara Malaysia, Kuala Lumpur, Malaysia. http://www.bnm.gov.my/index.php?ch=13&cat=banking/.

BU., 2015. Understanding authentication, authorization and encryption. Boston University, Boston, Massachusetts. http://www.bu.edu/tech/about/security-resources/bestpractice/auth/.

Belanger, F., J.S. Hiller and W.J. Smith, 2002. Trustworthiness in electronic commerce: The role of privacy, security and site attributes. J. Strat. Inform. Syst., 11: 245-270.

BolehVPN, 2013. How secure is your bank's website? Comparing Malaysian banks HTTPS security. BolehVPN, Switzerland,Europe. https://www.bolehvpn.net/blog/2013/10/28/how-secure-is-your-banks-website-comparing-malaysian-banks-https-security/.

Canstar, 2013. Commonwealth bank of Australia online. History of Online Banking in Australia, Australia, http://www.canstar.com.au/online-banking/history-of-Internet-banking/.

Chou D., C. and A.Y. Chou, 2000. A guide to internet revolution in banking, the E-commerce revolution. Inf. Syst. Manage., 17: 1-7.

CimbClicks, 2015. We view your security with utmost importance: Remember to always protect your devices. CIMB Clicks Malaysia, Malaysia. https://www.cimbclicks.com.my/ibk/.

Easy Solutions Inc., 2015. Best security practices in online banking platform. Easy Solutions, Inc., Doral, Florida. www.easysol.net/images/stories/downloads/Best_security_practices_online_banking.pdf.

FFIB., 2011. Authentication in an internet banking environment. Federal Financial Institutions Bank, Virginia, USA., https://www.ffiec.gov/pdf/authentication_guidance.pdf.

IU., 2014. What is authentication. Indiana University, Bloomington, Indiana. https://kb.iu.edu/d/alqk.

Investopedia, 2015. Online banking definition. World Trade Center, New York, USA., http://www.investopedia.com/terms/o/onlinebanking.

Jassal, R.K. and R.K. Sehgal, 2013. Online banking security flaws: A study. Intl. J. Adv. Res. Comput. Sci. Software Eng., 3: 1061-1071.

Katz, J., 2002. Efficient cryptographic protocols preventing man-in-the-middle attacks. Ph.D Thesis, Columbia University, New York City, USA.

Kelly, G. and M.B. Kenzie, 2002. Security, privacy and confidentiality issues on the Internet. J. Med. Internet Res., 4: e1-e12.

Liou, J.C. and S. Bhashyam, 2010. A feasible and cost effective two-factor authentication for online transactions. Proceedings of the 2010 2nd International Conference on Software Engineering and Data Mining (SEDM), June 23-25, 2010, IEEE, New Jersey, USA., ISBN: 978-89-88678-22-0, pp: 47-51.

Madhuravani, B. and P.B. Reddy, 2013. A comprehensive study on different authentication factors. Intl. J. Eng. Res. Technol., 2: 1358-1361.

Maybank2u, 2015. Build your online store with a secured payment gateway. Maybank2u. Malaysia. http://www.maybank2u.com.my/.

Prasad, M.V.N.K. and S.G. Kumar, 2015. Authentication factors for internet banking. Institute for Development and Research in Banking Technology, Hyderabad, India.

Preeti, R., 2014. Physical security: A biometric approach. Intl. J. Eng. Comput. Sci., 3: 3864-3868.

Steven, P., 2005. MyCERT: Less hacking, more phishing. Cyber Security Malaysia, Malaysia. http://www.cybersecurity.my/bahasa/knowledge_bank/news/2005/main/detail/895/index.html.

Suh, B. and I. Han, 2002. Effect of trust on customer acceptance of internet banking. Electron. Commer. Res. Applic., 1: 247-263.

Thigpen, S., 2015. Banking authentication: Authentication methods used for banking. CBH Technologies, Los Angeles California.

Warren, S.D. and L.D. Brandeis, 1890. The right to privacy. Harvard Law Rev., 4: 193-220.

Yang, Y.J., 2015. The security of electronic banking. National Institute of Standards and Technology, Gaithersburg, Maryland http://csrc.nist.gov/nissc/1997/proceedings/041.pdf.

Zaaba, Z.F. and T.K. Boon, 2015. Examination on usability issues of security warning dialogs. J. Multidiscip. Eng. Sci. Technol., 18: 26-35.

Zaaba, Z.F., S.M. Furnell and P.S. Dowland, 2014. A study on improving security warnings. Proceedings of the 2014 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M), November 17-18, 2014, IEEE, Penang, Malaysia, ISBN: 978-1-4799-6242-6, pp: 1-5.