Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/3149
DOI URL: http://dx.doi.org/10.21474/IJAR01/3149

RESEARCH ARTICLE

LEVEL OF USABILITY OF THE MULTI FACTOR AUTHENTICATION PROCESS OF ONLINE BANKING: A USER EXPERIENCE STUDY.

Gamage M. P.
Sri Lanka Institute of Information Technology (SLIIT), BoC Merchant Tower, Colombo 03, Sri Lanka.

Manuscript Info

Manuscript History

Received: 15 December 2016
Final Accepted: 10 January 2017
Published: February 2017

Key words:-
Website, Usability, Online banking, Internet, Authentication, MFA

Abstract

Most banks now offer their services online, which is known as online banking. Bank activities involve very sensitive information. Due to the high level of fraud banks have recently introduced a new authentication method which requires the users to provide more than one factor to authenticate themselves which is known as Multi Factor Authentication (MFA). But means of improving the security might compromise the level of usability of the website. Being a country with less IT literate people the researcher assumes that introduction of MFA might have an impact on the Sri Lankan online users. This paper presents an empirical study on the level of usability of MFA mechanisms used by Sri Lankan banks at present as experienced by the users. According to the results it was identified the number of online banking users are less in Sri Lanka, but they are accepting the MFA methods as usable.

Introduction:-

Most of the businesses have their own websites which provides their customers the ease of performing transactions from wherever they are. But when developing the website it is essential to check that the website furnishes to the purpose. Website users prefer websites that are convenient to use and in overall which provides them an appealing online experience. “On the Web, usability is a necessary condition for survival” [1]. “If a website is difficult to use, people leave. There's no such thing as a user reading a website manual or otherwise spending much time trying to figure out an interface. There are plenty of other websites available; leaving is the first line of defense when users encounter a difficulty” [1].

“Based on the principles of Human Computer Interaction (HCI), web usability has become a recognized success factor for all e-business, including online banking” [2]. When considering online banking websites to enhance user experience further and to attract more customers it is necessary to understand the level of usability of the bank website. Past research confirms that website navigation issues, security fears and ambiguity in content are the major concerns that user face [2-6]. According to the study it demonstrates that ultimate result of a bad user experience is 50% of customers registered for online banking disregarding the use of the website [2]. Also since Bank websites deal with sensitive information like username, passwords, credit card details, account information; they are one of those that make security a priority. When the banks try to improve the authentication process through more secure mechanisms it definitely has a negative impact on the level of usability. Therefore website usability and security can be claimed as the most vibrant issues in online banking.

Corresponding Author:-Gamage M. P.
Address:-Sri Lanka Institute of Information Technology (SLIIT), BoC Merchant Tower, Colombo 03, Sri Lanka.

Users are allowed to access their personal information through the website after an authentication process. So the security of the authentication process which serves as the entry point for the customer is extremely important.Banks have introduced Multi Factor Authentication (MFA) method in order to improve the security reassuring more online customers. MFA aims to improve the traditional password-based authentication method known as Single Factor Authentication (SFA) by demanding users to provide a supplementary authentication factor such as a separate transaction password or a verification code. When banks try to enhance security mechanisms it undeniably affect the level of usability of the website. So there is a tradeoff between the level of usability and security of a bank website.

Recently banks in Sri Lanka also started implementing this MFA method. Sri Lanka is a country with less Information Technology (IT) literate people. So this study aims to find out level of usability of the introduced MFA methods as perceived by the users and to analyze if it has greatly affected the usability than the SFA for the current online banking users.

The main objectives of the study are;

- Identify MFA methods introduced in online banking
- Find the level of usability of the available MFA methods
- Identify if the introduction of MFA has greatly affected the usability than the SFA

Literature Review:-

Online banking facility provides as an essential gateway for the banking customers to interact with their bank to get the services they need. In order to make the online experience a better one the banks should consider the level of usability of their websites. Also banks try to incorporate advanced security mechanisms to their online banking websites in order to reassure the customer to use the online facility without any fear of fraud. So the security and usability of online banking are a key concern. At present there are many researches which discuss the usability issues of bank websites [7-10].

The major problem with the definition of usability is that it is quite difficult to precisely explain the term. The most common explanation of usability is simplified to ease-of-use [1], [8]. In spite of many other definitions on usability, Jakob Nielsen's [1], [11] definition on web usability is extensively used by usability experts. Jakob Nielsen was named as "the reigning guru of web usability" by Fortune and as "perhaps the best-known design and usability guru on the Internet" by Financial Times [12]. Usability is defined by five eminence components by him as;

- Learnability: "How easy is it for users to accomplish basic tasks the first time they encounter the design?" [1].
- Efficiency: "Once users have learned the design, how quickly can they perform tasks?" [1].
- Memorability: "When users return to the design after a period of not using it, how easily can they reestablish proficiency?" [1].
- Errors: "How many errors do users make, how severe are these errors, and how easily can they recover from the errors?" [1].
- Satisfaction: "How pleasant is it to use the design?" [1].

The main gateway provided for security is the authentication process. So the banks try to improve their online banking authentication mechanisms more and more. But this definitely will have an impact on the level of usability of the online banking website. At present there are different authenticating mechanisms available [13] [14].

Traditional authentication or SFA uses one factor for user authentication on a website. Often it is a knowledge-based factor, such as a password which is set during the registration process. Ma and Feng have appraised the usability of three alternative authentication methods that are available; the text passwords, mnemonic passwords and graphical passwords [15]. According to the results presented text passwords and graphical passwords proved to be equally memorable [15] and that mnemonic passwords had a higher failure rate [15]. Also they identified that the use of graphical passwords consumed more time when compared to other types [15]. Theresults gathered through a questionnaire and in-depth interviews with 86 contributors were used by Nilsson to compare authentication using 'security box' method (one time password) and 'fixed passwords' method (password is preset) [16]. The results exposed that security boxes are perceived as more dependable by the users [16]. L. Gorman in his study compares passwords, security tokens, and biometrics and there possible combinations for MFA [17]. Different authenticating mechanisms in use as identified by him are;

- Knowledge-Based (what you know) - characterized by secrecy [17].
- Object-Based (what you have) – characterized by physical possession [17].
- ID-Based ("who you are") – characterized by uniqueness [17].

In the study done by Cristofaro et al. they conducted an online survey with 219 Mechanical Turk users, tomeasure the usability of diverse MFA methods [18]. The methods considered in the study are one-time codes generated by security tokens, one-time PINsreceived via SMS or email, and dedicated smartphone apps [18].They recorded contexts and motivations, and also considered theirinfluence on usability of different MFA methods. The study acknowledged that the existing differences among the usage of MFA methods be subject toindividualcharacteristics of people, more than the actual technologies orcontexts of use. [18]. Also the study result shows that users perceived MFA as usable [18]. According to the study done by Gunson et al. MFA methods were perceived as less usable but more secure than SFA methods [19].

All above studies discusses about different authentication methods and their usability of websites in general. This study focuses about the application of MFA methods only in the context of online banking.

The experiment conducted by Weir et al. used 50 e-banking customers to compare the security and usability of MFA methods when using token devices [20]. Through the research it was identified that participant felt card-activated tokens and the push button token to be usable and secure but the chip-and-PIN method to be less usable [20]. According to M. Mannanthe and P. C. Oorschot the guaranteed online transaction security applies only for the users who fulfill certain security requirements stated by the banks [21]. After examining some of the requirements set by major Canadian banks they evaluated on security aspects using 123 technically advanced users from a university environment. The results strongly supported their view about the gap between expectations of the bank and the actions of user related to security of online banking. [21]

When considering the importance to improve the security methods and at the same time the importance of not complicating the usability of the online experience this research tries to find the effect of applying MFA methods for Sri Lankan online banking users. The assumptions of the researcher are;

- MFA is still not popular in Sri Lankan banks
- MFA will be perceived as less usable
- SFA and MFA will have a big difference on the level of usability

Methodology:-

The sample considered for the survey are IT companies/institutes in Sri Lanka under the assumption that they would comprise people open to online activities such as online banking. Questionnaire Technique is used to collect data about the level of usability of the authenticating process, as well as to gather important feedback from online banking users. The questionnaire used for the analysis is created as an online survey questionnaire using an online questionnaire tool, and is emailed to the selected sample.

The first section of the questionnaire covers general data about respondents such as their gender, age, name of the bank and type of authenticating method used by the bank (SFA, MFA). To get an idea about the level of IT literacy factors like the length of time using computers, length of time using online banking services are counted. The second section, aims to collect the level of usability of the authenticating process. As the usability measurement technique the usability definition proposed by Jakob Nielsen is used. Accordingly the five usability characteristics considered are learnability, efficiency, memorability, errors and satisfaction [1]. A set of questions targets to address one of the characteristics (independent variables). User can rate a given question on a five-point Likert scale from 1 (strongly agree) to 5 (strongly disagree). The results obtained from these are used to get a measure on the level of usability (which is the dependent variable). Since online banking usually makes the user authenticate himself during different activities such as logging in, doing a money transfer, paying a bill, etc. for the study only one of the activities is considered. So the authenticating process used when 'performing a money transfer to a third party account' only is considered. The third section includes open-ended questions to capture additional particulars related to user authentication process.

Results and Discussion:-

According to the results obtained the number of online banking users in Sri Lanka is identified as only 39%. So it is identified that in Sri Lanka online banking users within the IT industry is still very small, proving the assumption of the researcher that IT job/study related people are very much exposed to online transactions through internet otherwise.

When considering the age 82% which is a significant percentage are included into the 20 – 39 years age category. It can be assumed that this bias of age factor is introduced because in Sri Lanka IT literacy is very less among older generation.

98% of the respondents who participated had used computers for more than five years and 70% had been using online banking for more than three years. This provides evidence that the users using the online facilities are the ones with a high level of IT literacy and skills.

According to the results it can be seen that majority of the users are clustered around only 5 banks for the online service. So for the study the authentication methods of those five banks are considered. The banks authentication methods when doing a money transfer to a third party account are limited to;

- Logging password only (40% banks)
- Logging password + Transaction password (which is pre set) (20% banks)
- Logging password + SMS/email based one-time verification code (20% banks)
- Logging password + token based code (20% banks)

Other authentication methods like graphical passwords and biometric identification are not used in banks in Sri Lanka. It can be due to reasons like images taking more time to load and the high cost involved in implementing biometric authentication.

According to the results during a transaction through online banking 60% of the banks use MFA and only 40% of the banks are using SFA. So it is identified that majority of banks in Sri Lanka have already applied MFA. When doing the analysis, level of usability for SFA and MFA is independently considered.

When considering the efficiency (second usability characteristic) in SFA, 78% users agreed that they can easily authenticate themselves without any trouble. But some have issues like confusion among their own passwords they have to use for different online systems, which made them successful only after the second attempt. According to the study outcomes out of the users who used MFA only 64% has agreed that they often log in without issues. This result indicates that some difficulty is there with MFA. From the open ended questions it is identified that the reason for above is mainly due to factors such as confusion between different passwords they had to use (separate logging password and transaction password), time taken to access their phone/mail to find out the verification code and forgetting to have the security code generator token.

According to the preliminary analysis of the data, majority of (81%) responded positively about the usability (dependent variable) of MFA while only 13% responded negatively. This result proves that users accept the MFA method. When considering the results of users who use banks with SFA method majority of users (89%) who use SFA responded positively, while only 8% responded negatively. When comparing the percentage of positive respondents for SFA and MFA the results shows that there is no significant difference between the two methods as perceived by the users.

Conclusion:-

This is an empirical study about the level of usability of the MFA mechanisms applied in online banking in the context of Sri Lankan banks. The study considered 95 online banking users in Sri Lanka who have long-term experience with the use of internet. The results show that still not all banks have applied MFA even with the huge rate of online fraud that happens. Even though the researcher thought MFA might have a big impact on the level of usability of the website it is proved otherwise. Users perceive MFA as usable and have accepted the use of the new method. Since there is no big difference between the percentage of positive respondents of MFA and SFA it can be recommended that banks should use MFA since it is more secure than the SFA. Due to the limited number of online banking users for the study only 95 user responses could be explored. In future can validate the results further by

enhancing the sample size and also by conducting a detailed analysis to check that the results obtained are truly related to the usability factor and not biased on the specific bank they used.

Acknowledgement:-

I present my earnest thanks to my family members for the reinforcement provided throughout the study. Also I would like to add my gratitude for all participants of the survey questionnaire for spending their valuable time in helping my research.

References:-

1. Jakob Nielsen. "Usability 101: Introduction to Usability", January 4, 2012. [Online]. Available: http://www.nngroup.com/articles/usability-101-introduction-to-usability/. [Accessed: Dec. 28, 2016].
2. Nikki Bochel, "User Friendly e-Banking". 25 April 2004. [Online]. Available: http://uservision.co.uk/2004/04/user-friendly-e-banking. [Accessed: Aug. 5, 2016].
3. Chris Nickson, "Why shouldn't you be banking online?", 2002, [Online]. Available: http://news.digitaltrends.com/feature/49/shouldn-t-you-bebanking-online. [Accessed: Aug. 20, 2015].
4. "Investigating Factors effecting users and non-users of using internet banking in Saudi Arabia". Doctoral Symposium, Brunel Business SchoolLondon, May 21 & 22, 2008.
5. P. B. Lowry, T. Spaulding, T. Wells, G. Moody, K. Moffit and S. Madariaga, "A Theoretical Model and Empirical Results Linking Website Interactivity and Usability Satisfaction," Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), 2006, pp. 123a-123a.
6. Gamage. M. P, Kodagoda. G. N. Level of Customer Satisfaction and Usability Issues in Online Banking Websites - published at: "International Journal of Scientific and Research Publications (IJSRP), Volume 3, Issue 1, January 2013 Edition".
7. P. Weichbroth, K. Redlarski and I. Garnik, "Eye-tracking web usability research," *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Gdansk, 2016, pp. 1681-1684.
8. M. Alhanahnah and D. Chadwick, "Boosting Usability for Protecting Online Banking Applications Against APTs," 2016 Cybersecurity and Cyberforensics Conference (CCC), Amman, 2016, pp. 70-76.
9. M. M. Althobaiti and P. Mayhew, "Usable security of authentication process: New approach and practical assessment," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 179-180.
10. Ranganathan S. &Rajee N. Usability Testing to Improvise Online-banking experience. 4th Annual International Software Testing Conference in India 2004. February 20 - 21, 2004. Le Meridien, Pune, India.
11. Jakob Nielsen, "Usability", 2004, [Online]. Available: http://www.useit.com/jakob/ . [Accessed: Sep. 5, 2015].
12. Jakob Nielsen, "Evidence-Based User Experience Research, Training, and Consulting", [Online]. Available: https://www.nngroup.com/people/jakob-nielsen/. [Accessed: Nov. 25, 2016].
13. Tweak and Trick. "The Most Common Authentication Methods Used Today." [Online]. http://www.tweakandtrick.com/2012/06/most-common-authentication-methods-used.html. [Accessed: Nov. 28, 2016].
14. Network World. "Seven strong authentication methods". [Online]. http://www.networkworld.com/article/2296774/access-control/seven-strong-authentication-methods.html. [Accessed: Nov. 28, 2016].
15. Ma, Y., &Feng, J. 2011. Evaluating usability of three authentication methods in web-based application. Ninth international conference on software engineering research, management and application. August 2011. Baltimore, MD.
16. Nilsson, M., Adams, A., & Herd, S. 2005. Building security and trust in online banking. In: Extended abstracts on human factors in computing systems (CHI '05). New York, NY, ACM Press, pp. 1701–04.
17. O'Gorman, L. 2003. Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE. 91(12), pp. 2019-2040.
18. De Cristofaro, E., Du, H., Freudiger, J., &Norcie, G. 2014. A Comparative Usability Study of Two-Factor Authentication. [Online] http://arxiv.org/abs/1309.5344v2 [Accessed: Aug. 5, 2015].
19. Gunson, N., Marshall, D., Morton, H., & Jack, M. 2011. "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking". Computers & Security. 30(4).
20. Weir, C.S., Douglas, D., Carruthers, M., & Jack, M. 2009. "User perceptions of security, convenience and usability for ebanking authentication tokens". Computers & Security, 28(1).
21. M Mannan, P. C. van Oorschot. 2007. "Security and usability: the gap in real-world online banking". NSPW '07 Proceedings of the 2007 Workshop on New Security Paradigms, Pages 1-14.