INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 11, ISSUE 5, MAY-2020
ISSN 2229-5518

Usability and Security in Internet Banking Password (Survey)

Tahir Mehmood, Dr. Ghulam Muhammad Shaikh
Department of Computer Science
Bahria University

Karachi, Pakistan

Abstract— *The aim of this paper is to analyze the importance of security and usability upon one and other in Internet Banking Password and how and why the people prefer security over usability or vice versa, taking the domain of passwords in internet banking we did the research and analysis of the preference of the user over usability or security in different scenarios during registration and login process in internet banking. Using survey results we can extract the optimum solution that will fulfill the user preferences accordingly which could be used to design the system according to the user needs.*

Keywords — Usability; Security; Survey; password; Internet Banking

I. INTRODUCTION

E-banking is the set of banking services delivered to the user via electronic interfaces. Access to services is provided by either of an automated teller machine (ATM), a computer, a mobile phone, or smartphones. E-banking allows users to purchase a variety of services such as balance and transaction consultation, request for financial documents, transfer of account-to-account money, making transfers, payment invoices, credit simulation and securities portfolio management. Thus, access to the banking package is fast, accurate, convenient and timely. The question of the adoption of e-banking by private users has been widely studied in the literature. despite the rapid emergence of e-banking, however, research into the adoption of e- banks by companies is rare [7].

There were almost 800 breaches of data in the United States in the year 2015 and all of these breaches were caused by hacked passwords. Users themselves make their accounts susceptible by reusing the same passwords on multiple sites

[9]. Today, businesses can do all their banking transactions electronically. The adoption of e-banking by banks facilitates the management of accounts, significantly reduces the management costs of all their banking operations, saves time, generates productivity gains and strengthens the relationship with the bank. In addition, e-banking makes it possible to secure transactions by eliminating the circulation of paper and reducing the risk of data loss. Thus, e-banking offers businesses, even small and medium-sized businesses SMEs, immeasurable benefits.

Talking in a more technical term there is no general equation for limiting the paradox amongst ease of use and security, programmers and security engineers (SAs) keep on facing the situation of these two apparently clashing objectives in building up a framework that is both usable and secure.

This means that the system is pretty easy to operate and effective for users to perform their tasks while making it hard for intruders to compromise. The relationship between usability design and security architecture, as guided by the mental model of the user and the designer, is vital for building usable and secure systems. However, the main challenge remains in how to elicit the users tacit knowledge and translate it into the interface design without compromising system security or underestimating system usability [1].

The principle challenge in outlining usable security is to carefully strike a harmony between shielding the framework from unapproved access and intellectually plan the policies to comply with the user's desires and fulfilment. Accomplishing such adjust isn't an easy task. Most present day policies are described by complex security interfaces to the degree that the user faces an issue of recognizing the security prerequisites. Along these lines, the creators suggested that the User Interface nearly coordinate the users' psychological models for guaranteeing a protected conduct. Something else, poor convenience may bring about low profitability as well as propels the users to bypass security controls [2].

II. BACKGROUND

The view of security is the prospect that users assume that their private info will not be viewed, archived and exploited in an inconsistent manner by inappropriate parties during the transfer and storage of data. Threats, attacks on data and system transactions, or unauthorized access to the

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 11, ISSUE 5, MAY-2020
ISSN 2229-5518

account through false authentication can be made in the context of e-banking. Users must feel secure when carrying out financial transactions [12].

A perception of security of the e-banking services lead the banks to value these services. Security improves value through perceived benefits. The more secure the services, the more important the functional benefits will be. It provides users safe banking, thereby reducing there psychological costs and gaining there trust. Similarly, if banking services are secure, they will be valued given their price [12]. People typically develop ineffective policies to reduce the cognitive load of password management for multiple accounts. As the number of accounts accumulated by an e-banking user increases, it turns into increasingly hard to maintain distinct passwords per account and handle every password according to the corresponding password policies [27].

III. LITERATURE OVERVIEW

A. Identification and Authentication

The method of identifying and validating the claims of users and procedures about themselves is Identification and Authentication. An IDA is typically used when deciding whether a user or a process can allow access to system resources. Determining who may have access to this or that data should be an integral part of the data classification process. [5]

Internet authentication has a number of problems. It is easy enough to intercept the identification and authentication data and repeat them to impersonate the user. When authenticating in general, users often express dissatisfaction with it and often make mistakes, which makes it possible to obtain data through social engineering. Another problem is the ability to wedge into a user session after they perform authentication.

There are three main types of authentication - static, strong and permanent. Static authentication uses passwords and other technologies that can be compromised by repeating this information to attackers. Often these passwords are called reusable passwords. Strong authentication uses cryptography or other methods to create one-time passwords that are used during work sessions. This method can be compromised by inserting messages by an attacker into the connection. Permanent authentication prevents attackers from inserting messages [13].

B. General Internet Authentication Policies

The following are general rules for working with passwords that are useful for using the Internet:

- User IDs and passwords must be unique for each user.

- Passwords must be any combination of eight alphanumeric characters (must not be names or known phrases).

- A “digit,” a “symbol”, an “uppercase English letter,” and a “lowercase English letter,” must be contained within the passwords [4].

- Credentials should be periodically tested by special programs to identify guessable passwords (these programs should have a set of rules for generating guessable passwords) [9].

- Administrators must save users credentials safely by implementing b-crypt, s-crypt, pbkdf2 or similar. Most administrators implement MD5 which is broken and thus insecure [10].

- Passwords should be kept secret, that is, should not be communicated to other people, should not be inserted into the texts of programs, and should not be written on paper.

- Passwords must be changed every 90 days. Most systems can force a password to be changed after a certain time and prevent the use of the same or guessable password [11].

- User budgets should be frozen after 3 failed login attempts.

- All cases of incorrectly entered passwords must be recorded in the system log so that actions can be taken later.

- User sessions with the server should be blocked after a 15-minute inactivity (or other specified period). To resume a session, the password must be entered again.

- Upon successful login, the date and time of the last login should be displayed.

- User budgets should be blocked after a certain period of non-use.

- For high risk system after a certain number of unauthorized access attempts, the system should give an alarm and give false server messages to the user who makes these attempts so that he remains connected to the system while the security administrator tries to find out his location [2].

C. Policy for strong authentication

There are many technologies for implementing robust authentication, including dynamic password generators, cryptography-based smart-card request-response systems, as well as digital signatures and certificates.

Researches shows that policies comprising of long passwords with fewer constraints are harder to crack than of small length passwords with strong policies. Users are responsible for the safe use and storage of all authentication devices given to them. Smart cards should not be stored with the computer used to access the computers of the organization. If a smart card is lost or stolen, users should

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 11, ISSUE 5, MAY-2020
ISSN 2229-5518

immediately inform the security service so that it can be blocked [5].

D. Electronic Signatures and Certificates

If electronic signatures are to be used for authentication, then the use of certificates is required. Certificates are issued by a responsible person or an external trusted organization. Within the Internet, several commercial infrastructures have emerged to distribute electronic signature certificates (PKI).

E. Object Based Passwords

Object based passwords transforms user-nominated digital objects to high-entropy text passwords. So Digital Objects are used instead of remembering exact passwords. Study shows that this pattern provides robust security with superior usability and outstanding memorability [10].

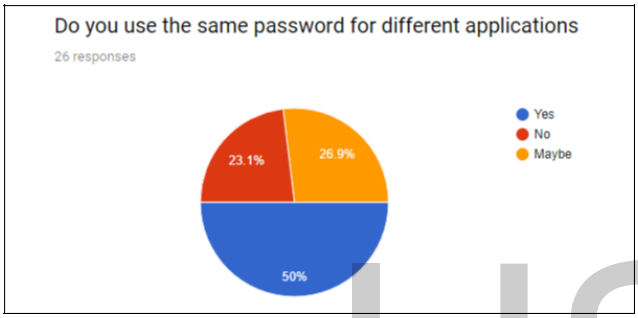

FIGURE 1: SAME PASSWORD FOR DIFFERENT APPLICATIONS

Mostly user selected YES shows users want to keep less number of passwords in their memory because it is difficult to memorize and manage more passwords so keeping same password for different applications is usable for the user but it is very insecure and may hazardous in case of the security.

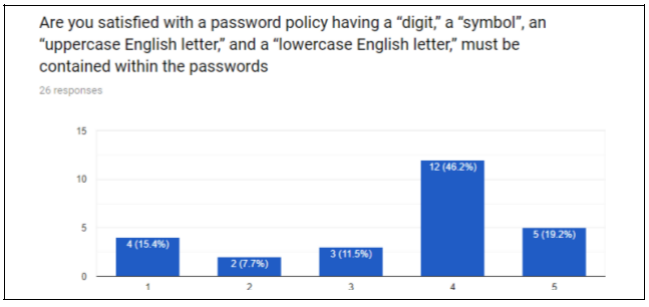

FIGURE 2: PASSWORD POLICY SATISFACTION

Mostly users are satisfied with the password policies having a digit, a symbol, an uppercase English letter, and a lowercase English letter. Some users are not happy with restrictions and complexities of the passwords required and some wants to remove the 2 factor authentications. They want the easiest way to create password which can quickly be memorized and should be secure enough.

IV. SURVEY

A survey is circulated to analyze the user preferences for the usability and security of application passwords. Survey is circulated in software Houses and Financial institutions. Participants were selected among the categories; Software Engineers and IT Professionals and organization's management. Survey is circulated in such a way that a questionnaire is given to the participants with a short overview about the concerned terminologies.

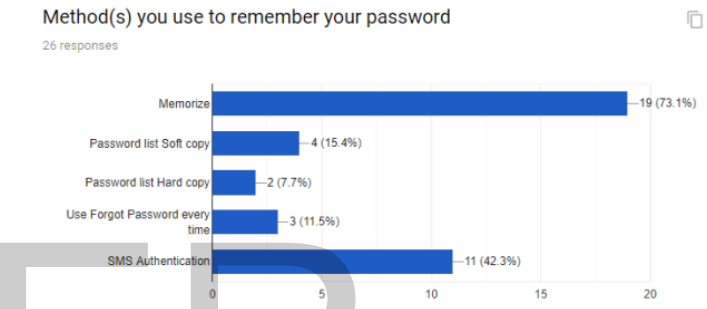

FIGURE 3: METHODS TO REMEMBER PASSWORDS

As there are lot of applications that requires username and passwords. Users prefer to memorize passwords rather than maintaining them in hardcopy or softcopy. Which is again not user friendly and due to complex password policies it becomes difficult to memorize in case mostly users forgot the passwords. Many of the users also prefer SMS authentication to be used as a medium for remembering and authenticating themselves to their e-banking accounts.

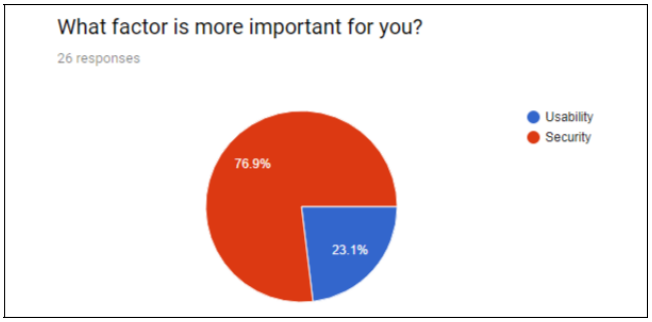

FIGURE 4: SECURITY VS USABILITY

Both the usability and security are important for the user but the system which is more secure with enough usability will be successful. Most of the users prefer Security over Usability.

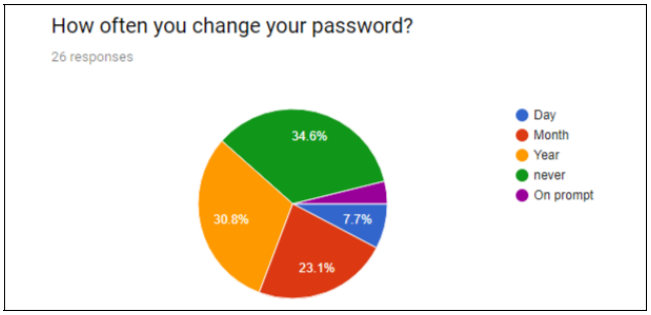

FIGURE 5: PASSWORD CHANGE FREQUENCY

Mostly users wants to keep away from changing the passwords as it requires user effort that is it is not user friendly way of securing the application, this should be done in such a way that user has do to do as less as possible efforts and gets the maximum secure application. Moreover changing passwords more frequently are often forgotten as compared to passwords with longer validity.

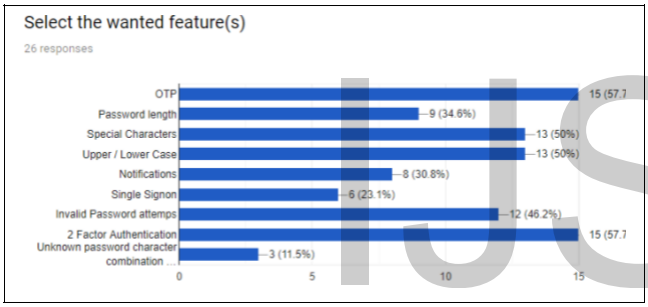

FIGURE 7: WANTED FEATURE

OTP and 2 factor Authentication appears to be very attracting for the user as it makes the transactions transparent, also tracking becomes easy and this also acts like a digital proof to the user. The mobile is a safety token for authentication. By entering the username and password, user login is the online banking account. For security purposes, separate token numbers are used to execute the banking operation, such as withdrawal of money, checking of the balance, etc. [16].

V. ANALYSIS

The following results have been concluded based on responses of the questionnaire.

Question	Results
Same password for different Application	Yes
Password policy satisfaction	No

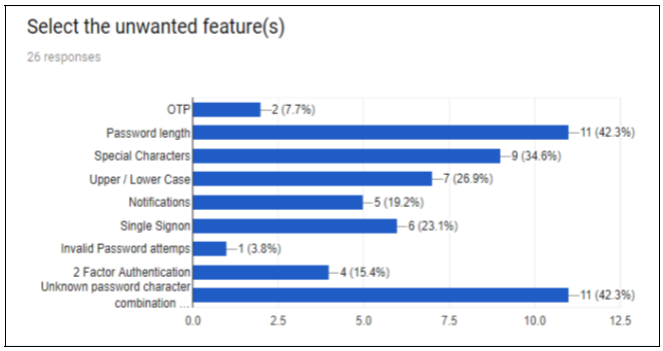

FIGURE 6: UNWANTED FEATURE

Uncommon passwords combination and password length policies seems to be the most unwanted features for the users find it difficult remembering the uncommon and fixed length passwords.

Usability verses Security	Security
Password change frequency	Never
Wanted features	OTP, 2 factor Authorization
Unwanted feature	Password Length
Forgot password frequency	Sometime
Password currently in Use	3 - 5
Methods to remember passwords	Memorize
Involvementof Object Based Passwords	Yes

It is also evident that the use of a single-factor authentication (e.g. password) in the Internet banking world is no longer considered secure. Easy to guess passwords such as name and date of birth are sure targets for automated password collection programs. So to meet the requirements of organizations to provide their users with a stronger and safer authentication process the two - factor authentication was introduced. [16]. Also invalid password attempts should be kept as low as possible to keep the application secure from hackers but human error is also the factor that conflict with it some banks are very strict in

setting invalid attempts policies which is very frustrating for the e-banking users as there is no chance of error for them which is also not user friendly way to secure the application [24-25].

It is difficult to achieve both security and ease of use in e - banking systems, as security is not a system feature that can be automatically provided while users focus on their primary goal of doing business with their bank [30]. In addition, password requirements information should be mandatory. Moreover, extended SSL validation certificates for improved customer confidentiality should also be considered. Education programs should be developed and implemented to raise awareness of security, such as information about potential risks and threats, for all existing and potential Internet banking customers, programs between banks, universities and government sectors. [27].

VI. CONCLUSION

Fromthe above literature overview and questionnaire analysis we have come to the point that in Pakistan, the attitude toward usability is not the only factor determining preference of an authentication process. In fact, majority of the users prefer security over usability because of emerging online security risks and attacks. So it is vital to understand that what factors impact upon users' perceptions of trust. Hence, the major challenge for online banking, is to maintain the balance for users between perceived trust, security and usability [29].

VII. FUTURE WORK

In future research, we will evaluate the personal password management behaviors associated with the storage of passwords by people and the protective measures employed. Instead of suggesting specific methods for the administration of passwords, we would like to give general advice on which methods to avoid and which methods to accept. The aim is to identify personal, user-friendly and secure password management methods. [18].

VIII. REFERENCES

[1] J. Chakraborty and N. Nguyen, The Effect of Simulation in Large-Scale Data Collection-An Example of Password Policy Development, Springer International Publishing, p270 2018

[2] J. C. &. J. D. Mona A. Mohamed, Trading off usability and security in user interface, p.25, 2017

[3] SANS Institute 2014, Password Protection Policy. url{https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy}

[4] Richard Shay et al., Can Long Passwords Be Secure and Usable?, p.34, May 2014

[5] John R. Vacca, Practical Internet Security url{https://dl.acm.org/citation.cfm?id=1951776} , p 77, 2010

[6] R. Wash, Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites," p. 14, 2016.

[7] P. Subsorna and S. Limwiriyakulb, A Comparative Analysis of Internet Banking Security in Thailand , Procedia Engineering 32 (p.260 – 272), 25 November 2011

[8] AlFayyadh, Thorsheim, Jøsang and Klevjer, Usability and Security of Texng Usability of Password Management with Standardized Password Policies, The Seventh Conference on Network and Information Systems Security, May 2012

[9] Telesign, Beyond the Password: The Future of Account Security, url{https://www.telesign.com/wp-content/uploads/2016/06/Telesign-Report-Beyond-the-Password-June-2016-1.pdf }, June 2016

[10] Biddle, Mannan, Oorschot, and Whalen, User Study, Analysis, and Usable Security of Passwords Based on Digital Objects, IEEE Transactions on Information Forensics and Security 6(3):970 - 979 , October 2011

[11] IDEXX Laboratories, Practice Management Software , Password Policy, 2015

[12] Elizabeth Stobert, Robert Biddle, The Password Life Cycle: User Behaviour in Managing Passwords, Tenth Symposium On Usable Privacy and Security,p.243, July 2014

[13] Kirk Hausman, Martin M. Weiss, Diane Barrett, CompTIA Security, Pearson IT Certification, Mar 6, 2015

[14] Judith Gebauer, Douglas Kline, Password Security Risk versus Effort:An Exploratory Study on User-Perceived Risk and the Intention to Use Online Applications, Journal of Information Systems Applied Research (JISAR), August 2011

[15] Hristo Bojinov, Elie Bursztein, Xavier Boyen, and Dan Boneh, Kamouflage: Loss-Resistant Password Management, Springer (2010)

[16] P.Y.Pawar, Sagar Acharya, Apoorva Polawar, Priyashree Baldawa, Sourabh Junghare, Internet Banking Two Factor Authentication Using Smartphone, International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013

[17] Joseph Bonneau, S¨oren Preibusch, Ross Anderson, A birthday present every eleven wallets?The security of customer-chosen banking PINs, International

Conference on Financial Cryptography and Data Security, 2012

[18] Bander AlFayyadh, Per Thorsheim, Audun Jøsang and Henning

Klevjer, Improving Usability of Password Management with Standardized Password Policies, The Seventh Conference on Network and Information Systems Security, 2012

[19] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay,Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Michelle L. Mazurek, Usability and Security of Text Passwords on Mobile Devices, CHI Conference on Human Factors in Computing Systems Pages 527-539, 2016

[20] JoshuaB. Gross, Mary Beth Rosson, Ruthie Berman, Understanding Password Choices: How FrequentlyEntered Passwords are Re-used Across Websites, 2016 USENIX Annual Technical Conference

[21] L. Tam , M. Glassman & M. Vandenwauve, The psychology of password management: a tradeoff between security and convenience, Behaviour & Information Technology Vol. 29, No. 3, May–June 2010, 233–244

[22] Philip G. Inglesant, M. Angela Sasse, The true cost of unusable password policies: password use in the wild, Proceedings of the SIGCHI Conference on Human Factors in Computing SystemsPages 383-392, Apr 2010

[23] Robert Biddle, Mohammad Mannan, Paul C. van Oorschot, and Tara Whalen, User Study, Analysis, and Usable Security of Passwords Based on Digital Objects, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 3, SEPTEMBER 2011

[24] Mike Wyatt, Irfan Saif, and David Mapgaonkar, A world beyond passwords - Improving security, efficiency, and user experience in digital transformation, Deloitte Review 2016

[25] Catherine S. Weira, Gary Douglas, Tim Richardson, Mervyn Jack, Usable security: User preferences for authentication methods in eBanking and the effects of experience, Interacting with Computers 22 (2010) 153–164

[26] Karen Scarfone , Murugiah Souppaya, Guide to Enterprise Password Management, NIST Special Publication 800-118, Apr 2016

[27] Sonia Chiasson, Robert Biddle, Anil Somayaji, Even Experts Deserve Usable Security: Design guidelines for security management systems, Symposium onUsable Privacy and Security July 2007.

[28] E. Stobert, The Password Life Cycle:User Behaviour in Managing Passwords, p. 13, 2014.

[29] Maria Nilsson& Anne Adams, Simon Herd, Building Security and Trust in Online Banking, Late Breaking Results: Posters, Apr 2007

[30] Morten Hertzum, Niels Jørgensen, Mie Nørgaard, USABLE SECURITY AND E-BANKING: EASE OF USE VIS-À-VIS SECURITY , AJIS Special Issue