The Impact of Awareness of Password Management of Digital Banking Services on Customer's Adoption in India

Nitin Bansal, Nishtha Pareek, Abhinav Nigam

Abstract: ***Password management is a highly decisive component while adopting digital banking services. Password composition strategies facilitate the users to construct a safe, secure and strong password which is difficult to crack and misuse your confidential information. There should be an institutional structure to enhance the awareness level of password management of users to minimize the probability of cyber attack. This study has focused on the analysis of impact of awareness of password management of digital banking services on customer adoption in India. To analyze the applicability and reliability of scale, factor analysis has been administered before the use of stepwise method (forward selection) of multiple regression. Primary data on 5 point Likert scale has collected from the Delhi region with the help of questionnaires through a self administered approach. Stratified random sampling technique was used and total 432 useful schedules were considered for analysis of data using SPSS version 23. The results of the study show that there is a positive impact of awareness of password management of digital banking services on customer's adoption in India.***

Keywords: Password security, Password management, Password composition strategy, Digital banking services, Common password, Awareness of password management, Cyber frauds

I. INTRODUCTION

Internet affects the life of individuals and corporate to a greater extent in present era. Now a days, internet is required at home as well as workplace to communicate, search information, banking and investments etc. Sometimes the functions performed by the users need privacy and individuals use passwords to secure their performed functions and information. Online security has become a challenge for the corporate, individuals, banking institutions, social networking websites and many more [1]. There are policies in the corporate and universities to educate the users regarding the password creation and on regular basis corporate remind the users to create and secure a strong password [10]. Focusing on the user is highly important because all the security functions would not protect the access to systems in case of mismanagement of passwords by its users [6]. People usually create a password which is easy to guess and having the similar passwords in multiple accounts. A weak password is an invitation of cyber fraud. A strong password must have minimum characters, composition of different characters and should be a combination of letters which is difficult to guess [13].

Revised Manuscript Received on June 22, 2020.

Nitin Bansal, Assistant Professor, FMS-WISDOM, Banasthali Vidyapith, Rajasthan, India

Nishtha Pareek, Assistant Professor, FMS-WISDOM, Banasthali Vidyapith, Rajasthan, India

Abhinav Nigam, Assistant Professor, FMS-WISDOM, Banasthali Vidyapith, Rajasthan, India

Corporate allocates huge amount of funds to install the safeguards to protect access to their systems and technology. Many corporate spend huge amount of funds to educate the users to minimize the cyber frauds. Most of the banking institutions enhance digital literacy of its customers to enhance the trust level of the customers and minimize the probability of unwanted financial transactions [2].

II. LITERATURE REVIEW

Password Management Strategies

Password composition policies helped the users to create a strong password to protect the access to their systems. Strong passwords require minimum characters in passwords, the composition of characters, character classes, and understanding the impact of password blacklist, which prevent the users to create a highly common password. The purpose of all these tools is to help the users to create a less vulnerable to automated password guessing [11]. People usually having different strategies to create password. One common strategy is to reuse the password across different accounts. The main objective to follow this strategy is to remember the password easily as on regular basis one individual uses over 20 passwords in their daily lives [18], [19]. Users usually do not remember the passwords of their multiple accounts. Most of the users write down their password of different accounts as a common practice. Through this strategy users need not to memorize the passwords of their varying accounts and whenever users need the access, they easily found it. But this strategy having high risk to access their accounts by unauthorized person in case of misplace of their notebooks where the passwords were written [9]. Use of the common passwords depends on the user, who is having multiple accounts. If user needs multiple passwords, then it's a common practice to reuse the same password for varying accounts [7].

III. PASSWORD UPDATION CHALLENGES

Forced to change password might not change the attitude of the users to create a strong password. It is observed that most of the users replace the new password with the common characters of the old password, which enhance the probability of cyber crime. It is also observed that repeating security advice causes users to internalize it, even if evidence supporting the advice is scant [10]. Every month users should change the passwords of their accounts to defeat the cyber attacks.

There is a need to revise the password composition policy as the time has changed now. At the time when the password composition policies were proposed first time, computational power was far scarcer than it is now and a successful password cracking attack would have taken several months. Further password expiration might act as a failsafe mechanism to eventually lockout attackers who may have gained access to a legitimate user's password without having knowledge [17]. Users exactly reused the passwords for 67 percent of their accounts and the passwords used in different accounts having minimum four common characters by 79 percent of participants in survey [14]. 20 percent of the websites protect the accounts of its users by unauthorized access through the password expiration strategy. These websites regularly required to update the passwords [5]. Prior studies revealed that update password on regular basis having negative implications for usability as most of the users update their passwords which is similar to their old password. Only 30 percent of the users create an entirely new password whenever it is required to update [16].

Password Security Perception

Perceptions of users about password security studied and observed that users have misunderstanding about the password strength and security. Users think that adding digits made their password stronger than it really did. There is a mismatch between the user's perception about the password security and the user's password creation strategy [19]. Users usually create password that does not match their desired security level. Create a weak password for high valued account is having high risk [20]. Behaviour of users to create password such as users having knowledge about the password security, strong password generation strategies, use of varying characters in password studied and observed that most of the users usually do not follow the strong password composition strategies even after they are having knowledge and intention to create a strong password [15].

IV. RESEARCH GAP

Awareness of password management is a crucial component to trust on the digital banking services. After a through literature review it is revealed that most of the significant studies have concentrated on the various aspects of password security but they were lacking on the customer's awareness aspect about the password management in India which is having impact on the customer's adoption of digital banking services. In today's world it is essential to educate the users about the password composition strategies to reduce the cyber attacks, which leads to the enhancement of customer's adoption of digital banking services.

Objectives

a. To identify the customer's awareness level of password management of digital banking services in India.

b. To analyse the impact of awareness of password management on the customer's adoption of digital banking services in India.

This research paper has studied the impact of awareness of password management on customer's adoption of digital banking services which leads to the enhancement of effectiveness and efficiency of customers as well as banking institutions.

V. RESEARCH METHODOLOGY

Data collection

For the collection of primary data, questionnaires and schedules were used through a self administered approach. Schedules were administered to 500 customers in Delhi region. Delhi is the national capital of India and having the customer base of all segments.

Sampling Method

For this study, stratified random sampling technique has been considered to ensure the representation of different segments of the total population.

Sample Size

To obtain the useful 384 questionnaires and schedules from the respondents, 500 questionnaires and schedules were administered. Out of which 432 useful questionnaires and schedules were obtained of different socio-economic profile.

Reliability

Cronbach's alpha was used to check the reliability of the responses. The value of Cronbach's alpha was found to be above 0.5 for all the variables (Table 7), which is good.

Normality

To ensure the normality of the data, Skewness and Kurtosis were also checked (Table 4) and the results are within acceptable range i.e. between -2 to +2 [8].

Tools for analysis

In this study, data was analysed using stepwise method (forward selection) of multiple linear regression, after factor analysis was used. The collected data has been processed for analysis using SPSS version 23.

Data Analysis

This paper is divided in two sections, as follows:

1. Customer's password management awareness level

In this section customer's password management awareness level has been identified. The respondents were asked 8 questions (Five Point Likert Scale, Table 1) ranging from password awareness to various aspects of password management.

Table 1: Variables coding for customer's awareness level of password management

Variable Details	Variable Name	Nature
Password management	ID_1	Independent
Alpha numeric aspect	ID_2	Independent
Minimum characters	ID_3	Independent
Varying characters	ID_4	Independent
Expiry period	ID_5	Independent
Common password	ID_6	Independent
Served saved password	ID_7	Independent
Intimation of password Expiry	ID_8	Independent

Binary	-	(Recorded variable to judge awareness of password management)

The responses to various questions were than recomputed into a separate variable using SPSS, to calculate composite password management awareness level.

Table 2: Binary

	Frequency	Valid %	Cumulative %
Adequate Awareness Level	168	38.89	38.89
Low Awareness Level	264	61.11	100.0
Total	432	100.0	100.0

This new variable (Binary) was also on Five Point Likert Scale.

After this the response for the new variable ranging from strongly disagree to neutral are recorded as 0, that is low awareness level of password management and responses from partially agree to strongly agree are recorded as 1 that is adequate awareness level of password management (Table 2).

As can be seen from Table 2, out of 432 customers, only 168 customers (38.89%) have adequate awareness level of password management, remaining 264 customers (61.11%) have low awareness level of password management.

There are several factors responsible for these low levels.

(a) Indian customers usually avoid adopting digital banking services because of fear factor, so they also avoid learning the password management.
(b) Rarely there is any organized institutional structure to enhance the awareness level of customers about password management.
(c) People usually like to create a password which is easy to memorize and intentionally not intended to know about password management.

2. Impact of awareness of password management on Customer's adoption

Various practical aspects of customer's awareness level of password management and its impact on customer's adoption of digital banking services are analyzed. The respondents were asked 8 questions (Five Point Likert Scale, Table 3)

Table 3: Variables coding for awareness level of password management's influence on customer's adoption

Variable Details	Variable Name	Nature
Customer's adoption	D_1	Dependent
Knowledge_Password management	ID_{11}	Independent
Password Management Strategies	ID_{12}	Independent
Updation_Password	ID_{13}	Independent
Server saved password	ID_{14}	Independent
System saved password	ID_{15}	Independent
Trust enhancement	ID_{16}	Independent
Risk reduction	ID_{17}	Independent
Enhancement_Password Awareness	ID_{18}	Independent

Based on extensive literature review and personal interaction with the bank's customers following hypotheses were formed for analyzing the impact of awareness of password management of digital banking services on customer's adoption:

H_{01}: In the presence of other predictors there will be no impact of awareness of password management on the customer's adoption level of digital banking services.

H_{02}: In the presence of other predictors there will be no impact of password composition strategies on the customer's adoption level of digital banking services.

H_{03}: In the presence of other predictors there will be no impact of regular updation of password on the customer's adoption level of digital banking services.

H_{04}: In the presence of other predictors there will be no impact of server saved password on the customer's adoption level of digital banking services.

H_{05}: In the presence of other predictors there will be no impact of system saved password on the customer's adoption level of digital banking services.

H_{06}: In the presence of other predictors there will be no impact of high trust factor through password management on the customer's adoption level of digital banking services.

H_{07}: In the presence of other predictors there will be no impact of low risk factor through password management on the customer's adoption level of digital banking services.

H_{08}: In the presence of other predictors there will be no impact of enhancement of password management awareness on the customer's adoption level of digital banking services.

To the testing of hypotheses, stepwise method (forward selection) of multiple regression has been used. This method analyzes the effect of predictors entered at each step. This provides a better picture of influence of each predictor entered in previous step in presence of new predictor.

Table 4: Normality Analysis

Descriptive Statistics

	N	Mean	Skewness	Kurtosis
	Statistic	Statistic	Statistic	Statistic
D_1	432	3.78	-.501	-.401
ID_{11}	432	3.02	.016	-1.313
ID_{12}	432	3.23	-.127	-1.045
ID_{13}	432	2.86	-.076	-.993
ID_{14}	432	3.20	-.329	-1.123
ID_{15}	432	3.78	-.501	-.401
ID_{16}	432	3.55	-.707	.399
ID_{17}	432	3.38	.417	-.986
ID_{18}	432	3.07	-.094	-1.414
Valid N (listwise)	432			

Table 4 of the Descriptive Statistics found that all the values of all the variables are well as these are having values of skewness and kurtosis in the range of -2 to +2 which is acceptable [8].

Factor Analysis

Table 5: KMO and Bartlett's Test

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.725
Bartlett's Test of Sphericity	Aprox. Chi-Square	2770.356
	df	86
	Sig.	.000

Table 5 of KMO and Bartlett's Test is showing that the KMO value is 0.725, which is nearer to 1.0. Hence the value is acceptable and justifies the appropriateness of factor analysis [12].

Table 6: Rotated Component Matrix

Rotated Component Matrix[a]

	Component		
	1	2	3
ID_{11}	.902		
ID_{12}	.854		
ID_{13}		.847	
ID_{15}		.746	
ID_{16}		.630	
ID_{17}			.839
ID_{18}			.783

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 4 iterations.

To analyse the applicability of the scale, exploratory factor analysis was administered (Table 6). To identify the underlying factors, principal component analysis with varimax rotation was used. As a result of factor analysis, 3 components revealed, which covered 71.830 % of variability and independent variable ID_{14} has been excluded because its impact on the component was 0.259 which is less than the minimum acceptable range.

Table 7: Scale reliability

Variables/combined items	Anchor	Cronbach's α
1	2	0.842
2	3	0.793
3	2	0.718

All the three components have Cronbach's α value more than 0.7 which is considered well [3].

Multiple Linear Regression

Table 8: Model Summary [d]

Model	R	R Square	Adjusted R Square
1	.720[a]	.518	.514
2	.872[b]	.760	.758
3	.823[c]	.677	.675

a. Predictors: (Constant), ID_{11}

b. Predictors: (Constant), ID_{13}, ID_{15}, ID_{16}

c. Predictors: (Constant), ID_{17}, ID_{18}

d. Dependent Variable: D_1

Table 9: ANOVA

Model		*Sum of Squares*	*df*	*Mean Square*	*F*	*Sig.*
1	Regression	195.441	3	65.147	142.429	.000[b]
	Residual	182.044	428	0.457		
	Total	377.485	431			
2	Regression	597.917	3	199.306	419.524	.000[c]
	Residual	189.080	428	0.475		
	Total	786.998	431			
3	Regression	504.664	3	168.221	278.387	.000[d]
	Residual	240.500	428	0.604		

Total	745.164	431

a. Dependent Variable: D_1
b. Predictors: (Constant), ID_{11}
c. Predictors: (Constant), ID_{13}, ID_{15}, ID_{16}
d. Predictors: (Constant), ID_{17}, ID_{18}

Table 10: Coefficients[a]

Model		*Unstandardized coefficients*		*Standardized coefficients*		
		B	*Std.Error*	*Beta*	*t*	*Sig.*
1	(Constant)	0.666	0.154		4.323	0.000
	ID_{11}	0.335	0.048	0.325	7.018	0.000
2	(Constant)	-0.389	0.103		-3.766	0.000
	ID_{13}	0.331	0.038	0.292	8.811	0.000
	ID_{15}	0.578	0.046	0.519	12.526	0.000
	ID_{16}	0.167	0.042	0.158	3.927	0.000
3	(Constant)	-0.168	0.122		-1.37	0.000
	ID_{17}	0.35	0.054	0.297	6.492	0.000
	ID_{18}	0.405	0.048	0.361	8.397	0.000

a. Dependent Variable: D_1

Table 11: Excluded Variables

Excluded Variables[a]

Model		Beta In	t	Sig.	Partial Correlation	Collinearity Statistics
						Tolerance
1	ID_{12}	.084[d]	1.804	.072	.090	.550

a. Dependent Variable: D_1

d. Predictors in the Model: (Constant), ID_{11}

VI. REGRESSION ANALYSIS

Firstly the effect of predictors entered in the model 1, 2 and 3 were analysed. For the testing of hypotheses stepwise method (forward selection) of multiple linear regression has been used. These are the consolidated tables of all the models. Initial tables have been omitted for clarity.

In model 1 hypotheses H_{01} and H_{02} are simultaneously analysed and it can be seen from the model summary (Table 8) that the model explains 51.8% of the total variation of the dependent variable customer's adoption (variable D_1).

ANOVA (Table 9), explains that the model is significant ($p<.001$).

From the coefficients table (Table 10), it can be seen that ID_{11} has significant value ($p < 0.05$) thus we reject the null hypotheses H_{01} and accept the alternate hypotheses H_{a1}.

To further analyse these outcomes regression equation is created as follows:

$D_1 = 0.666 + 0.325*ID_{11}$ (Equation 5.1)

$H_{a1:}$ In the presence of other predictors, there will be significant impact of knowledge of password management on the customer's adoption level.

As is apparent from the equation 5.1, one unit change in ID_{11} will result in 0.325 unit change in the knowledge of password management level of customers.

In model 2 hypotheses $H_{03,}$ H_{05} and H_{06} are simultaneously analysed and it can be seen from the model summary (Table 8) that the model explains 76.0% of the total variation of the dependent variable customer's adoption (variable D_1).

ANOVA (Table 9), explains that the model is significant ($p<.001$).

From the coefficients table (Table 10), it can be seen that ID_{13}, ID_{15} and ID_{16} has significant value ($p < 0.05$) thus we reject the null hypotheses $H_{03,}$ H_{05} and $H_{06.}$

To further analyse these outcomes regression equation is created as follows:

D_1 = -0.389 + 0.292*ID_{13} + 0.519*ID_{15} + 0.158*ID_{16} (Equation 5.2)

$H_{a3:}$ In the presence of other predictors, there will be significant impact of regular updation of password on the customer's adoption level.

As is apparent from the equation 5.2, one unit change in ID_{13} will result in 0.292 unit change in regular updation of password by customers.

$H_{a5:}$ In the presence of other predictors, there will be significant impact of system saved password on the customer's adoption level.

As is apparent from the equation 5.2, one unit change in ID_{15} will result in 0.519 unit change in system saved password by customers.

$H_{a6:}$ In the presence of other predictors, there will be significant impact of trust enhancement through password management on the customer's adoption level.

As is apparent from the equation 5.2, one unit change in ID16 will result in 0.158 unit change in trust enhancement level through password management.

In model 3 hypotheses H_{07} and H_{08} are simultaneously analysed and it can be seen from the model summary (Table 8) that the model explains 67.7% of the total variation of the dependent variable customer's adoption (variable D_1).

ANOVA (Table 9), explains that the model is significant ($p<.001$).

From the coefficients table (Table 10), it can be seen that ID_{17} and ID_{18} has significant value ($p < 0.05$) thus we reject the null hypotheses H_{07} and H_{08}.

To further analyse these outcomes regression equation is created as follows:

D_1 = -0.168 + 0.297*ID_{17} + 0.361*ID_{18} (Equation 5.3)

$H_{a7:}$ In the presence of other predictors, there will be significant impact of risk reduction aspect through password management on the customer's adoption level.

As is apparent from the equation 5.3, one unit change in ID_{17} will result in 0.297 unit change in risk reduction aspect through password management.

$H_{a8:}$ In the presence of other predictors, there will be significant impact of enhancement of password management awareness on the customer's adoption level.

As is apparent from the equation 5.3, one unit change in ID_{18} will result in 0.361 unit change in enhancement of password management awareness level.

Excluded Variables: Variables ID_{12} has excluded on the basis of multiple linear regression analysis as the significance value of ID_{12} is 0.72 which is above 0.05 and in these cases null hypotheses i.e. H_{02} is accepted.

VII. CONCLUSION

The study started with an objective to analyze the impact of awareness of password management of digital banking services on customer's adoption. The result of the study can be seen from the above analysis and discussion that there is a positive effect of awareness of password management on customer's adoption. Awareness enhances the effective and efficient utilization of digital banking services. Through awareness enhancement programme, the risk probability of cyber attacks may be reduced which leads to the high level of trust of the customers. Then finally customers would be agreed to adopt digital banking services.

RECOMMENDATIONS

Following recommendations are made based on the analysis:
1. To enhance the awareness of password management, there should be institutional structure which regularly works upon to enhance the awareness level.
2. Password management awareness programme should also be organized by the government of the country.
3. Banking institutions should also organize password management awareness programme on regular basis for its customers and non-customers.

REFERENCES

1. Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610-613.
2. Bishop, M. (1991, February). Password management. In *Compcon* (pp. 167-169).
3. Cavana, R. Y., Delahaye, B. L., & Sekaran, U. (2001). *Applied business research: Qualitative and quantitative methods.* John Wiley & Sons Australia.
4. Cranor & Egelman, S. (2011, May). Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2595-2604). ACM.
5. Florencio, D., & Herley, C. (2007, May). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (pp. 657-666). ACM.
6. Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27-35.
7. Gaw, S., & Felten, E. W. (2006, July). Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security* (pp. 44-55). ACM.
8. George, D. and Mallery, P. (2010) *SPSS for Windows Step by Step: A Simple Guide and Reference 17.0* Update. 10th Edition, Pearson, Boston.
9. Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256-267.
10. Habib, H., Naeini, P. E., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Christin, N., & Cranor, L. F. (2018). User behaviors and attitudes under password expiration policies. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)* (pp. 13-30).
11. Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, N., Christin, L.F.,
12. Malhotra, N. (2008). Marketing Research – An Applied Orientation (5th ed.). New Delhi: Pearson Education.
13. Malone, D., & Maher, K. (2012, April). Investigating the distribution of password choices. In *Proceedings of the 21st international conference on World Wide Web* (pp. 301-310). ACM.
14. Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L.F., Egelman, S., & Forget, A. (2017, October). Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 295-310). ACM.
15. Riley, S. (2006). Password security: What users know and what they actually do. *Usability News*, *8*(1), 2833-2836.
16. Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., & Cranor, L. F. (2010, July). Encountering stronger password requirements: user attitudes and behaviours. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 2). ACM.
17. Spafford, E. (2006). Security myths and passwords. *CERIAS Blog*, *19*.
18. Stobert, E., & Biddle, R. (2014). The password life cycle: user behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)* (pp. 243-255).

19. Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N., & Cranor, L. F. (2015). " I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*(pp. 123-140).
20. Zhang-Kennedy, L., Chiasson, S., & van Oorschot, P. (2016, June). Revisiting password rules: facilitating human management of passwords. In *2016 APWG symposium on electronic crime research (eCrime)* (pp. 1-10). IEEE.