



## Password Knowledge versus Password Management Practice

### A case Study Federal University of Technology, Minna

Victor N. Adama<sup>1</sup>, Noel Moses Dogonyaro<sup>2</sup>, Victor L. Yisa<sup>3</sup>, Baba Meshach<sup>4</sup>, Ekundayo Ayobami<sup>5</sup>  
vnadama@fuminna.edu.ng, moses.noel@futminna.edu.ng, victor.yisa@futminna.edu.ng, babameshach01@futminna.edu.ng,  
a.ekundayo@futminna.edu.ng

**Abstract**— User authentication is one of the most important security characteristics of any system given today’s globalized digital life style. The safety and security of sensitive data, privacy and also critical infrastructure relies primarily on authentication. Amongst all authentication schemes, text-based passwords are the most deployed across various platforms, thus the importance of evaluating user password management practice cannot be overemphasized. This research via a case study aimed at establishing the theoretical password knowledge in comparison to actual password management practice of staff and students from Information Technology (IT) inclined departments of the Federal University of Technology, Minna. Results from the survey reveal that the target respondents are knowledgeable on good password management policies. However, actual password practice results by the respondents showed that they do not comply and effectively implement the theoretical password knowledge they possess. Thus it can be concluded that there is a significant difference between what respondents know compare to their actual practice. Numerous implications abound when this is the case as it makes users more vulnerable to security risks of unauthorized access by unauthorized users.

**Keywords**- Authentication; Password; Password knowledge; Password practice.

#### I. INTRODUCTION

In today’s digital age, people use the internet for business transactions, leisure and entertainment (social media), academics and many more. This has led to the dependency on computers and other computing devices (such as smart Phones, portable Document Adapter PDA, tablets, smart watches etc). According to Ritó, “The internet and digital technologies are transforming our world in every walk of our private and commercial lives” [1]. The task of keeping user data secure either offline or online is more than ever before of utmost importance. Data must be protected from unauthorized access (hackers for example), who can steal or manipulate them. One way to achieve this protection is through authentication. Authentication verifies the identity of the acclaimed user. However, there is the challenge in making authentication systems both secure and usable for authorized users. This is a trade-off that must be balanced.

Passwords play a vital role in our day-to-day lives. The traditional and most widely used method of authentication is the use of text passwords [2]. Passwords are used by users to gain access to personal computers, email accounts, mobile

phones, automated teller machines, bank accounts, work place networks and devices etc. They act as a gateway between the user and their personal information [3]. Good password policies recommend that users choose strong passwords. When adhered to, it decreases the chances of them easily guessed by unauthorized users. In contrast to these policies, the vast majority of users use weak passwords. In addition, they exhibit practices detrimental to their security. Such practices include writing passwords down in a book, using the exact same password across multiple accounts [4] and many others.

Blanchard in 2014 revealed that having weak passwords put millions of bank accounts and other financial transactions on the internet at high risk of being hacked [5]. Helkala and Bakas found that most computer users were still found of using password that has guessable structure behind [6]. For example, a password that has just words or numbers and no combination of alphanumeric characters. A report by TeamsID in 2016, revealed twenty-five (25) most commonly used passwords [7]. The top two most commonly used passwords were “123456”, “password”, and “12345678”. Based on the report, further investigation revealed that most of the passwords were just “word” and numeric passwords making them easier to be guess unauthorized users.

This research is divided into various sections. Section II discusses password management and related works. Section III discusses research design. Section IV presents the survey results findings. Finally, conclusions and recommendation are presented.

#### II. RELATED WORKS

Several surveys have been conducted as regard to passwords. An example of such work is that of Stobert, and Biddle. Their work investigated how users cope with password requirements and management issues [8]. Also, the work of [9] revealed that if a user has N distinct passwords for each with a bit size  $\log(S)$ , then the user will have to remember not only  $N \times \log(S)$  bits, but also which of the  $N!$  mapping of password to account is correct. This gives a total expected bit size to be remembered of:

$$E(N) * \log(n!) \quad (1)$$

The factorial term quickly grows large as N increases. This is one of the reasons why many users ignore security

advice of having strong passwords to secure their personal data. Also, Notoatmodjo conducted a survey-based research on user passwords [10]. The research findings revealed that participants reported an average of 12.9 account and 8 passwords. It also revealed that the number of accounts was correlated to the user's number of years of internet experience. The researcher asked users to classify their accounts into high and low importance accounts groups and found that their categorization was related to the length of password, and how they were reused. Another research by Florencio et.al conducted a survey using 45 undergraduate respondents in which respondents were asked how many passwords they had and how often they reuse their passwords, how they handled Automated Teller Machine (ATM), Point of Sales (PoS), receipts and their knowledge on the use of passwords[11]. It was realized that users have a high number of reused passwords. Also, many have been scammed due to improper disposal of their ATM or PoS receipts and that most users rely on memory and passwords reminder features to remember their passwords. Research by Kelley et.al measured password strength against password cracking algorithms, testing the metrics for password creation policies [12].

However, while extensive studies have been conducted on passwords, there has been limited research done regarding the gap between the knowledge and behavior of password management [13]. In order to secure personal and organizational information, users of I.T tools need to know the importance of good password management. According to Stobert and Biddle, passwords go through a four (4) phase cycle [8]. This includes: creation, storage, maintenance, and deletion. This will be discussed in the following subsection.

#### A. Password Creation Phase

The first line of defense against unauthorized access to vital computer and personal data is to have a strong password. The stronger the password, the lower the chances it will be hacked [14]. The report showed that strong passwords must adhere strictly to various rules relating to password length and contents. A good password should have a combination of letters, numbers, and symbols.

#### B. Password Storage Phase

According to University of Illinois, using the same password for all accounts is like having one key that unlocks every door in a person's life [15]. Using the same password for multiple accounts is disastrous, because it would not take long for a hacker to identify which sites they can apply their hacked password on. In this regard, users can make use of password managers to store their passwords if they have many passwords that they utilize. A password manager is a database which stores user's passwords and their corresponding user accounts. The danger is that, if a hacker gains access to the master password, then, he or she (the hacker) would gain full control over all other user account [16]. By implication the master password must be highly secure. Password managers on their part are risky when used. They are no substitution for secure and usable authentication [4].

#### C. Password deletion

The work of Stobert and Biddle, revealed that most users tend to forget their passwords because they are too difficult to recall. If a user is no longer using an online account, he should delete the account and the corresponding password. When such accounts are left online over a period of time without been used, there is the tendency that a hacker can compromise the account for his selfish gain that could lead to identity theft.

### III. RESEARCH DESIGN

The research was carried out primarily based on a survey. The research aimed at investigating the existence of a gap between password policy knowledge and actual practice by IT users. The target audience in this research is limited to students and staff of the Federal University of Technology Minna with emphasis on Information Technology inclined departments. However other interested members from other departments who showed interest were allowed to participate. The research simply asked two research questions. First, are users knowledgeable on good password management policies? Secondly, do they put this knowledge into practice? Finally, to investigate the existence of the gap, a comparison between their theoretical knowledge and their actual password practice was carried out. This informed the survey to be structured and categorized into 3 sections. The first section collected information about the demographics of the respondents and their basic password needs. The second section, sought to establish the respondents theoretical password policy knowledge. Lastly the third section sought to establish the respondent's actual password behavior and practice.

Section 1: Demographics: In this section the survey collected basic information on the respondents and their basic password needs. The questions in table 1 are labeled using section number and question number, S1Q1 representing Section 1 Question 1.

TABLE I. DEMOGRAPHICS

Questions	Question Description
S1Q1	What is your gender?
S1Q2	Are you a student or a staff?
S1Q3	What is your course of study or what department do you work with?
S1Q4	What device(s) do you employ the use of passwords?
S1Q5	What online service(s)/account(s) do you have that requires the use of passwords on?

Section 2: Theoretical password policy knowledge: In this section the survey aimed at establishing the respondent's theoretical password policy knowledge. The questions in table 2 are labeled using section number and question number, S2 Q1 representing Section 2 Question 1.

TABLE II. THEORETICAL PASSWORD POLICY KNOWLEDGE QUESTIONS

Questions	Question Description
S2Q1	Have you received guidance on password creation in the past?
S2Q2	If "Yes" Where or from Whom?
S2Q3	What do you feel should be the minimum character length of a password?
S2Q4	What do you feel a password should be made up of?
S2Q5	Do you feel a password should contain symbols? for example @ ! \$ < # _ & % etc
S2Q6	How frequently do you feel users should change their passwords?
S2Q7	Do you feel users should delete their online accounts when they are no longer in use?
S2Q8	Should users write down their passwords on notes, in text files, etc.?
S2Q9	Briefly describe what a good password should contain

Section 3: Actual Password Practice: In this section the survey aimed at establishing the actual password behavior of the respondents. A Likert scale ranging from 1 to 5 was used for certain questions as shown in Table 3, where 1 stood for "always", 2 stood for "yes", 3 stood for "sometimes", 4 stood for "no" and 5 stood for "never". The questions in table 3 are labelled using section number and question number, S3Q1 representing Section 3 Question 1.

TABLE III. ACTUAL PASSWORD PRACTICE QUESTIONS

Questions	Question Description
S3Q1	Do you reuse old password you had earlier used?
S3Q2	Do your passwords only contain plain text with no special symbols such as numeric and alphanumeric characters?
S3Q3	Are your password lengths less than 10 characters?
S3Q4	Have you ever used the same password across multiple accounts/device(s)?
S3Q5	Have you ever used '12345' or 'password' for a password?
S3Q6	Have you ever used family member names, usernames and personal dates as passwords?
S3Q7	Have you ever used dictionary words as passwords?
S3Q8	How often do you change your passwords?
S3Q9	Which of the following statements is best suited to describe how you remember your passwords?
S3Q10	Do you write your passwords down?
S3Q11	If "Yes" where do you write your passwords down?
S3Q12	Do you share your passwords?
S3Q12	If "Yes", who do you share them with?
S3Q14	Do you delete your online accounts if you have not used them for a long time?
S3Q15	Do you reuse your regular passwords on accounts/services that you think should be extra protected?

#### IV. SURVEY AND FINDINGS

This section reports on the results and findings of the survey. The respondents consisted mainly of students and staff under IT inclined departments; however other interested members from other departments who showed interest were allowed to participate. Students who participated ranged from 100 level students (1st year) to postgraduate students.

The survey captured a total of 481 respondents. It comprised of 72 (15%) 100 level students, 79 (16.4%) 200 level students, 70 (14.6%) 300 level students, 89 (18.5%) 400 level students, 96 (20%) 500 level students, 18 (3.7%) Postgraduate Student and 57 (11.9%) Staff.

##### A. Theoretical Password Knowledge

Section 2 of the questionnaire aimed at establishing the theoretical knowledge of respondents as it regards passwords policies. The Table 4 summarizes responses to the questions asked in this section.

TABLE IV. THEORETICAL OPTIONS N=481

Questions	Yes	No	I don't Know
S2Q1	352 (73.2%)	90 (18.7%)	39 (8.1%)
S2Q5	295 (61.3%)	162 (33.7%)	24 (5%)
S2Q7	376 (78.2%)	88 (18.3%)	17 (3.5%)
S2Q8	191 (39.7%)	275 (57.2%)	15 (3.1%)

For S2Q1, 352 (73.2%) of the respondents stated having received guidance on creating passwords. For S2Q5, 295 (61.3%) of the respondents were of the opinion that passwords should contain symbols, whereas 162 (33.7%) respondents said "No" and 24 (5%) respondents stated that they did not know. For S2Q7, 376 (78.2%) respondents were of the opinion that online accounts should be deleted if not being used, whereas 88 (18.3%) stated they should not. For S2Q8, 275 (57.2%) respondents were of the opinion that passwords should not be written down, whereas 191 (39.7%) respondents stated users should write down their passwords and 15 (3.1%) respondents stated that they did not know. Table 5 summarizes responses from other theoretical password knowledge questions the survey asked.

TABLE V. THEORETICAL QUESTIONS RESULTS N=481

Questions	Option 1	Option 2	Option 3	Option 4	Option 5
S2Q2	While Studying	Websites/ Newspaper	From Friends	Other	
	109 (27.9%)	174 (44.6%)	49 (12.6%)	58 (14.9%)	
S2Q3	6	7	8	9	10
	163 (33.9%)	29 (6%)	237 (49.3%)	11 (2.3%)	41 (8.5%)
S2Q4	Uppercase letters	Lowercase Letters	Combination of both	Don't Know	
	3 (0.6%)	26 (5.4%)	443 (92.1%)	9 (1.9%)	
S2Q5	Every 90 days	Every 120 days	Never	Don't Know	

Questions	Option 1	Option 2	Option 3	Option 4	Option 5
	220 (45.7%)	64 (13.3%)	92 (19.1%)	105 (21.8%)	

Questions	Scale					Total	Average
	1	2	3	4	5		
S3Q15	20 (20)	55 (110)	46 (138)	173 (692)	176 (880)	1317	2.73

As shown in Table 5, For S2Q2, 109 (27.9%) respondents stated they received password guidance while studying, 174 (44.6%) from websites or newspapers and 49 (12.6%) received guidance from friends.

For S2Q3, 163(33.9%) respondents were of the opinion that the minimum number of characters should be 6, 29 (6%), that the minimum number of characters should be 7, 237 (49.3%), that the minimum number of characters be 8, 11(2.3%), that the minimum number of characters should be 9 and 41 (8.5%), that the minimum number of characters should be 10.

For S2Q4, 3 (0.6%) respondents felt a password should be made up of upper case letters, 26 (5.4%) respondents felt a password should be made up of lower case, 443 (92.1%) respondents felt a password should be made up of combination of both and 9 (1.9%) respondents did not know what passwords should be made up of.

For S2Q6, 220 (45.7%) respondents felt a password should be changed every 90 days, 64 (13.3%), respondents felt a password should be changed every 120 days, 92 (19.1%) respondents felt a password should never be changed and 105 (21.8%) did not know if password should be changed. For the open-ended question, S2Q9, most of the respondents indicated that a password should contain a combination of uppercase and lowercase characters, numbers and special characters. Based on these results, it is clear that the respondents are equipped with the necessary theoretical knowledge with regard to good password management.

**B. Actual Password Practice**

This section discusses the results and findings relating to the actual password practice of students and staff. Table 6 lists the questions which were asked using a 5-point Likert Scale where 1 = “always”, 2 = “yes”, 3 = “sometimes”, 4 = “no”, and 5 = “never”. Questions not using the 5-point Likert Scale are left out from this table and discussed later.

TABLE VI. LIKERT SCALE QUESTIONS N=481

Questions	Scale					Total	Average
	1	2	3	4	5		
S3Q1	1	2	3	4	5	1300	2.70
S3Q2	69 (69)	133 (266)	175 (525)	60 (240)	40 (200)	1652	3.43
S3Q3	34 (34)	66 (132)	94 (282)	186 (744)	92 (460)	1317	2.73
S3Q6	57 (57)	157 (314)	136 (408)	82 (328)	42 (210)	1512	3.14
S3Q7	44 (44)	148 (296)	62 (186)	109 (436)	110 (550)	1840	3.82

Table 6 shows the average for the questions asked in section 3. It made use of a 5-point Likert Scale response option. In the table above, an average of higher or equal to 4.0 indicates good password practice. However as can be observed all fall (Average of S3Q1, S3Q2, S3Q3, S3Q6, S3Q7, S3Q15) below 4.0 (that 2.70, 3.43, 2.73, 3.14, 3.82, 2.73 respectively). Therefore, no good password practice was observed across our respondents. Questions with an average of less than 3.0 indicate fairly poor practice. From Table 6 it can be observed that the respondents had poor practice when it comes to reuse of old password they had earlier used, their password lengths were less than 10 characters and indulge in the use of regular passwords to protect those accounts which require extra protection.

For S3Q1, 69 (14.5%) respondents stated they “always” reuse their password whereas 40 (8.4%) respondents stated they “never” reuse their passwords. For S3Q2, only 92 (19.5%) respondents said their passwords were “never” plaintext only, whereas 34 (7.2%) respondents’ passwords were “always” plaintext. For S3Q3, 57 (12%) respondents stated that their passwords were “always” less than 10 characters, 136 (28.7%) respondents indicated “sometimes”. For S3Q6, only 110 (23.3%) respondents stated that they “never” use personal dates and family member names as passwords. For S3Q7, only 176 (37.4%) respondents said they “never” use dictionary words as passwords, and for S3Q15, only 57 (12.2%) respondents stated that they “never” use their regular password in the accounts they think should be extra protected.

For S3Q4, 378 (79.7%) respondents have used the same password for multiple accounts. Similarly, for S3Q5, 362 (76.1%) respondents said “No” to this question. This is a good sign and shows that a large number of people do not use such simple passwords. For S3Q8, 40 (8.4%) respondents indicated that they change their passwords every 120 days and 148 (31.2%) respondents do not change their passwords. For S3Q8, 121 (25.5%) respondents change their passwords every 90 days. For S3Q12, 332 (70.9%) respondents do not share passwords. For S3Q14, 276 (58.7%) respondents do not delete their online accounts if they have not used them in a long time.

**V. DISCUSSION OF THE SURVEY RESULTS**

This section discusses the results and findings from the survey and compares the theoretical password knowledge with the actual password practice of respondents. There are a number of theoretical password knowledge questions, as were seen in Table 2, which can be correlated to the actual password practice questions, as seen in Table 3. Table 7 lists the theoretical and practice related questions that can be correlated.

TABLE VII. CORRELATION BETWEEN THEORETICAL PASSWORD KNOWLEDGE QUESTION AND ACTUAL PASSWORD PRACTICE QUESTIONS

Characteristic	Theoretical Password Knowledge Questions	Actual Password Behavior Questions
Password characteristics	S2Q4	S3Q2
Changing passwords	S2Q6	S3Q8
Delete online accounts	S2Q7	S3Q14
Writing passwords down	S2Q8	S3Q10

Figure 1 represents the respondents' theoretical password knowledge compared to their actual password management practice. For these results, only the top most answered questions are represented.

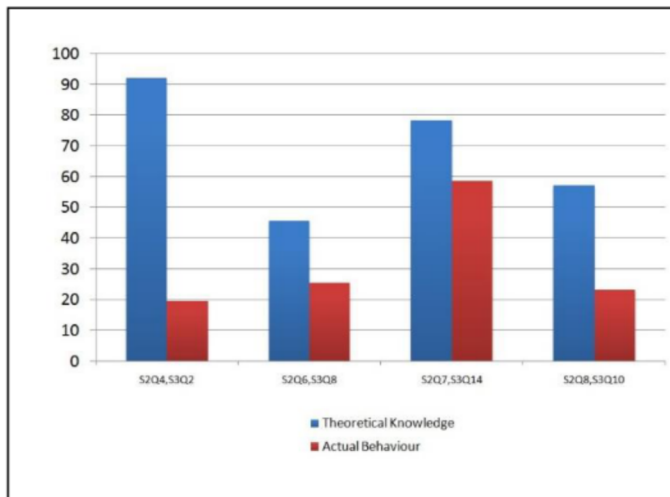


Figure 1. Theoretical password knowledge versus actual password practice of respondents.

As can be observed in Figure 1, there is a significant difference between the respondent's theoretical password knowledge and their actual password practice.

In S2Q3 and S3Q3, which referred to the minimum password length, it can be observed that the respondents know what the minimum average length should be for a password but when it comes to actual practice they do not adhere to what they know.

When asked what passwords should be made up of in S2Q4, 443 (92.1%) of the respondents were of the opinion passwords should be made up of a combination of upper case and lower case letters. This implies they are well aware of the policies that strong passwords should be complex (combination of upper, lower, special characters). However, when asked if their passwords only contain plain text with no special symbols such as numeric and alphanumeric characters in S3Q2, only 92 (19.5%) said never. This implies when it comes to actual practice, less than 20% of the respondents adhere to the policy. This was in contrast to 92.1% that know strong passwords should be a combination.

When asked how frequently they feel passwords should be changed in S2Q6, 220 (45.7%) of the respondents were of the view that passwords be changed at least every 90 days. However, when asked how often they change their passwords in S3Q8, only 121 (25.5%) said they do every 90 days. On the other hand, 148 (31.2%), (almost as much as those that do every 90 days) said they never change their passwords and 166 (34.9%) do not even know if passwords should be changed. Thus, only a few frequently change their passwords in practice.

When asked if they feel account users should delete their online accounts when they are no longer in use in S2Q7, 376 (78.2%) of the respondents were of the opinion that online accounts should be deleted when they are no longer in use. However, when asked if they delete their online accounts they have not used for a long time in S3Q14, 276 (58.7%) said they do not. This implies it makes sense to them that online accounts no longer in use be deleted, yet over half the sample respondents do not use this theoretical knowledge in practice.

When asked in S2Q8 if users should write down their passwords on notes or in text files, 275 (57.2%) said they do write down their passwords on notes or in text files. However, 110 (23.2%) admitted to writing down passwords and another 111 (23.4%) admitted to doing so sometimes. This implies although over 57% know it is bad practice to write down their passwords, close to half the sample population still write down passwords.

When asked in S3Q4 if they use the same password across multiple accounts/device(s), 378 (79.7%) said yes regardless of the obvious down sides of doing so. As earlier discussed they know what a strong password should look like yet rather find it more convenient using the same password across multiple accounts, devices and services. This is even more an issue as was established by S3Q15 when asked, "Do you reuse your regular passwords on accounts/services you think should be extra protected?" There 73 (15.6%) admitted they always reuse regular passwords on such accounts, 149 (31.8%) said Yes and 95 (20.3%) admitted they sometimes reuse regular passwords on accounts/services they know should be extra protected.

## VI. CONCLUTON

User authentication is one of the most important security characteristics of any system given today's globalized digital life style. The safety and security of not only sensitive data, privacy but also critical infrastructure relies primarily on authentication. Amongst all authentication schemes, text-based passwords are the most deployed across various platforms thus the importance of evaluating user password management practice cannot be overemphasized. Following the theoretical password knowledge findings and results from the survey conducted, it can be observed that the target respondents are knowledgeable on good password management policies. However, actual password practice results show they do not comply and effectively implement the theoretical password knowledge they possess. Thus it can be concluded that there is a significant difference between what respondents know compared to their actual practice. Numerous implications abound when this is the case as it makes users more vulnerable to security risks of unauthorized access by unauthorized users. This research

survey was limited to students and staff of the Federal University of Technology Minna with emphasis on Information Technology inclined departments. The results are not to be generalized but are however consistent with that of a study conducted by [13] in South Africa.

#### RECOMMENDATION

There clearly exists no “short cuts” to ensuring user safety and security as it concerns authentication. From the research findings, text based password pose a memorability problem that will continuously compel user to employ unsecured means of handling passwords. The need on that note, for an alternative to text passwords cannot be overemphasized. Graphical passwords are a relatively new scheme that tackles the memorability problem faced by the text based scheme. This is because users can remember images more easily than text. Despite the advantages Graphical passwords have to offer, they are yet to be widely deployed for online products and services. This may be because proposed Graphical passwords thus far only provide theoretical entropies between 12 and 23 bits which is far from the 39 to 53 bits offered by the text-based schemes. We recommend further and more extensive research into enhancing graphical password entropies as they possess the potential to replace text passwords.

#### REFERENCES

- [1] E. Ritó, Élhetőbb város–avagy “Smart City= Smart cities for a better world”. *KÖZÉP-EURÓPAI KÖZLEMÉNYEK*, 2018 2(41), 42-53.
- [2] A. De Angeli, L. Coventry, G. John, and K. Renaud, “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems” *International Journal of Human Computer Studies*, 2005, 63 (1-2), 128-152 doi.10 1016/iibcs.2005 04 020
- [3] M. McDowell, S. Heman & J. Rafail, “Security Tip(ST04002): Choosing and Protecting Passwords. US-CERT” [online]. 2013, Available at: <https://www.uscert.gov/ncas/tips/ST04-002> [Accessed 9 May, 2018]
- [4] K. Renaud, P. Mayer, M. Volkamer, and J. Maguire, “Are graphical authentication mechanisms as strong as passwords?In *Computer Science and Information Systems (FedCSIS)*, 2013 Federated Conference on 2013 Sep 8 (pp. 837-844). IEEE.
- [5] J. Blanchard, “Weak passwords put millions at risk of bank accounts and other information being hacked online mirror.2014 Available at: <http://www.mirror.co.uk/news/technologyscience/technology/weak-passwords-put-millionsrisk-4439460> [Accessed 25 March, 2018]
- [6] K. Helkala, and H. T. Bakás, “Extended results of Norwegian password security survey”, *Information Management & Computer Security*, 2014 22(4), pp.346-357.
- [7] TeamsID. “Worst Passwords Of 2015”.. Available at: <https://www.teamsid.com/worst-passwords-2015/>. 2016 [Accessed on 10 March. 2018]
- [8] E. Stobert, and R. Biddle, “The password life cycle: user behaviour in managing passwords.” In *Symposium On Usable Privacy and Security (SOUPS)*, Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance, 2014, pp. 243
- [9] G. Notoatmodjo, “Exploring the weakest link: A study of personal password security.” Master’s thesis, The University of Auckland, New Zealand, 2014.
- [10] University of Illinois. Why you should use different passwords. University of Illinois. 2014 Available at: <https://security.illinois.edu/content/why-you-should-usedifferentpasswords> [Accessed 30 April,2018]
- [11] D. Florencio, C. Herley, and P.C. van Oorschot, “An Administrator’s Guide to Internet Password research. In proceedings of the 28th USENIX large Installation System administration conference, 2015, pp. 35-52. USENIX Association.
- [12] P. G. Kelley, S. Komanduri, M. M. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor. “The impact of length and mathematical operators on the usability and security of one-time PINs” In *Financial Cryptography and Data Security*, Springer, 2013 pages 34–51.
- [13] D. T. Fredericks, L. A. Futcher and K., Thomson. “Comparing Student Password Knowledge and behavior: a case Study”. Proceedings of the Tenth International Symposium on Human aspects of Information and assurance (HAISA 2016). Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, port Elizabeth, South Africa. 2016.
- [14] Microsoft, “Maximum password age”. 2013 Available at: [https://technet.microsoft.com/enus/library/hh994573\(v=ws.10\).aspx](https://technet.microsoft.com/enus/library/hh994573(v=ws.10).aspx) [Accessed April, 2018]
- [15] University of Illinois, Why you should use different passwords. University of Illinois. 2014 Available at: <https://security.illinois.edu/content/why-you-should-usedifferent-passwords> [Accessed 30 April,2015]
- [16] S. Chaisson, A. Forget, E. Stobert, P.C. Oorschot, and R. Biddle, “Multiple password interference in text passwords and click based graphical passwords”. In *Proceedings of the 16th ACM conference on Computer and communications security 2009 Nov 9 (pp. 500-511)*. ACM.