Comparing Student Password Knowledge and Behaviour: A Case Study

D.T. Fredericks, L.A. Futcher and K.Thomson

Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
e-mail: {s212212435, Lynn.futcher,Kerry-lynn.thomson}@nmmu.ac.za

Abstract

Passwords have been around for a long time, but today more than ever, users have to remember many passwords for different accounts As a result, users tend to create simple passwords to access their accounts. When users create simple passwords they do not realise the possible repercussions that may arise. Statistics show that many data breaches have happened over the years because of poor password management. This paper discusses the importance of good password management. Passwords go through a lifecycle including creation, storage, maintenance and deletion. At each phase of the lifecycle, users should understand what is required to ensure good password management. In addition, this paper provides the results of a survey carried out at a university in South Africa. The survey took the form of a questionnaire and was distributed to Information Technology students ranging from 1st to 4th year. The aim of the survey was to determine student knowledge and their behaviour with regards to password management. The results and findings from the survey indicated that the respondents are educated with regards to good password management. However, it was discovered that not all users are putting that knowledge into practice, which highlights a significant vulnerability regarding their password behaviour.

Keywords:

Password management, password knowledge, password behaviour

1. Introduction

Passwords play an important role in everyday lives. They are used to log into personal computers, email accounts, bank accounts and company computers. Passwords act as a protective barrier between the user and their personal information (McDowell *et al*, 2013). Therefore, users should choose strong, secure passwords to protect their personal information from attackers. Many people, however, are still generating weak passwords and exhibiting bad practices, such as writing their passwords down or using the same password for multiple accounts (Renaud *et al*, 2013). Having weak passwords also puts bank accounts, and other information, at risk of being hacked (Blanchard, 2014). Often when users generate their passwords they have a guessable structure behind them. An example would be passwords that just have words or numbers for passwords and no combination of alphanumeric characters (Helkala, 2011). To further emphasise that users generate weak passwords, Splashdata released its annual list of the 25 most common passwords found amongst users. In this report, the *top three* most common passwords were

"123456", "password" and "12345678". Based on the report, a further finding was that most of the passwords were "word" passwords and numeric passwords, making them easier to guess. This could put user and company information at risk (TeamsID, 2016).

This paper discusses password management, firstly, by detailing related work in Section 2, and then discussing the importance of good password management in Section 3. Section 4 describes the design of the questionnaire while Section 5 presents the survey results and findings which are further discussed in Section 6. Finally, the paper is concluded in Section 7.

2. Related work

A number of related surveys have been conducted with regard to passwords. Gaw and Felten (2006) conducted a survey with 49 undergraduate respondents where the respondents were asked how many passwords they had and how often they reuse their passwords. From this survey, it was determined that users have a high number of reused passwords and that users rely heavily on memory and password reminder features to remember their passwords. From the results, it was determined that as respondents progress through their year of studies, they use more online accounts and they would reuse passwords more often (Gaw & Felten, 2006).

Additional studies have been done, measuring password strength against password cracking algorithms (Kelley *et al*, 2012) and testing metrics for password creation policies (Weir *et al*, 2010). However, while extensive studies have been conducted on passwords, there has been limited research done regarding the gap between the knowledge and behaviour of users with regards to password management.

3. Importance of good password management

In order to protect their personal and organizational information, users need to know the importance of good password management. According to Stobert and Biddle passwords go through a cycle of four phases (Stobert and Biddle, 2014) including: Creation, Storage, Maintenance and Deletion as discussed in the following subsections.

3.1. Creation Phase

Having a strong password provides a line of defence against unauthorised access to one's computer and personal information. The stronger the password, the lower the chances of users getting hacked and being exposed to malicious software (Microsoft, 2015). According to various sources (Microsoft, 2015; Apple, 2013; Google, 2016) strong passwords should adhere to various criteria relating to password length and content. For example, a combination of letters, numbers and symbols. In addition to the recommended criteria, various other tips are available to help users create strong passwords.

3.2. Storage Phase

According to the University of Illinois (2014) "*using the same password for all of your accounts is like having one key that unlocks every door in your life*". If users use the same password for multiple accounts, it would not take long for a smart hacker to identify which sites they can use these hacked passwords on. Users can make use of password managers to store passwords if they have many passwords that they utilize. A password manager is a database which stores users' passwords and usernames for different sites (Li *et al*, 2014). However, Chiasson *et al* mention that password managers have drawbacks as they typically use a master password for all user accounts. If the attacker gains access to the master password, then the attacker would gain full control over the user accounts (Chiasson *et al*, 2009). Renaud et al (2013) state that "*password managers are no substitution for a secure and usable authentication*". Password managers can be used, but users must understand that there are risks involved. Examples of password managers include LastPass, RoboForm, My1login and PasswordBox.

3.3. Maintenance Phase

Microsoft's password policy states that a best practice on the maximum password age should be between 30 and 90 days depending on the environment. By changing a password, an attacker has a limited amount of time in which they can compromise a user's password (Microsoft, 2012). According to Apple (2016), users should change their passwords regularly and avoid reusing passwords. One of the characteristics of strong passwords is that people should create passwords different from previously used passwords. If users want to update their passwords, they should create a brand new password.

3.4. Deletion Phase

Stobert and Biddle (2014) mention that users tend to forget passwords because of lack of memorability. If a user is no longer using an online account, it should be decided whether to keep it or delete it. There are risks involved if users decide to keep their accounts even though they are not using that specific online account. Such accounts can be compromised by hackers even though they do not use that account anymore because their personal information is stored (Schofield, 2013). To avoid this from happening, users should delete accounts if they have not used their accounts for a considerable period of time

4. Questionnaire design

The aim of the survey was to determine the students' theoretical knowledge with regard to good password management compared to their actual password behaviour. The survey was divided into 3 sections: Section 1 addressed the demographics, Section 2 focused on the theoretical password knowledge and Section 3 addressed the actual password behaviour of the respondents. Each section had multiple

questions. Most questions were closed questions with restricted options available. These options are indicated in brackets in Tables 1 and 2.

Section 1: Demographics: This section required the respondents to indicate their current year of study.

Section 2: Theoretical password knowledge: The purpose of this section was to determine the respondents' theoretical knowledge relating to good password management.

Q	Question description
Q2.1	Have you received guidance on password creation in the past? (Yes, No)
Q2.2	If 'Yes' Where or from Whom? (While studying, Websites/Newspaper, From friends or Other)
Q2.3	In your opinion, what should be the minimum character length of a password? (6, 7, 8, 9, 10)
Q2.4	In your opinion, a password should consist of (Uppercase letters, Lowercase Letters, Combination of both)
Q2.5	In your opinion, should a password contain symbols e,g @,!,$,<,#,? (Yes, No, Don't know)
Q2.6	How often should users change their password? (Every 90 days, Every 120 days, Never, Don't know)
Q2.7	Should users delete their online accounts if they are not using them? (Yes, No, Don't know)
Q2.8	Should users write down their passwords on notes, in text files, etc.? (Yes, No, Don't know)
Q2.9	Briefly, describe what a good password should contain. (Open ended)

Table 1: Theoretical password knowledge questions

The results of these questions are discussed in Section 5.2

Section 3: Actual password behaviour: The purpose of this section was to determine the respondents' actual password behaviour. A Likert scale ranging from 1 to 5 was used for certain questions as shown in Table 2, where 1 = '*always*', 3 = '*sometimes*' and 5 = '*never*'. The results of the Likert scale questions are shown in Table 5.

Q	Question description
Q3.1	Do you reuse your password over a period of time? (1 to 5)
Q3.2	Do your passwords only contain plaintext (no special symbols and alphanumeric characters) (1 to 5)
Q3.3	Are your password lengths less than 10 characters? (1 to 5)
Q3.4	Have you ever used the same password for multiple accounts e.g FaceBook, Gmail, NMMU account? (Yes, No)
Q3.5	Have you ever used `12345` or `password` for a password? (Yes, No)
Q3.6	Have you ever used family member names, usernames and personal dates as passwords? (1 to 5)
Q3.7	Have you ever used dictionary words as passwords? (1 to 5)
Q3.8	How often do you change your passwords? (Every 90 days, Every 120 days, Never, Don't know)
Q3.9	Which of the following statements is best suited to describe how you remember your passwords? (Often remember, Reset if cannot remember, Remember, Other)
Q3.10	Do you write your passwords down? (Yes, No, Sometimes)
Q3.11	If 'Yes' where do you write your passwords down? (In a text file, On a note, Password Manager, Don't know, Other)
Q3.12	Do you share your passwords? (Yes, No)
Q3.13	If 'Yes', who do you share them with? (Family, Friends, Colleagues, Peers)
Q3.14	Do you delete your online accounts if you haven't used them in a long time? (Yes, No)
Q3.15	Do you reuse your regular passwords in the accounts/services that you think should be extra protected? (1 to 5)

Table 2: Actual password management behaviour questions

The results of these questions are discussed in Section 5.3

5. Survey results and findings

This section reports on the results and findings of a survey carried out at a university in South Africa. The respondents consisted of IT students ranging from 1st year to 4th year.

5.1. Demographic results

The survey had a total of 45 respondents. In terms of the year of study, there were 5 (11%) 1st Years, 10 (22%) 2nd Years, 16 (36%) 3rd years and 14 (31%) 4th years.

5.2. Theoretical password knowledge

Tables 3 indicates responses to the (Yes, No) questions in Section 2 of the questionnaire.

Question	Yes	No	Don't know
Q2.1	34	11	0
Q2.5	29	12	4
Q2.7	29	10	6
Q2.8	4	39	2

Table 3: Theoretical options (n=45)

For Q2.1, 34 (75%) respondents stated having received guidance on creating passwords. For Q2.5, 29 (64%) respondents suggested that a password should contain symbols, whereas 12 (26%) respondents said *'No'* and 4 (8%) respondents stated that they '*Don't Know'*. For Q2.7, 29 (64%) respondents suggested that online accounts should be deleted if not being used. For Q2.8, 39 (86%) respondents stated that passwords should not be written down, whereas 4 (8%) respondents said *'Yes'* that users should write down their passwords.

Table 4 below represents theoretical password knowledge questions results. The greyed out options indicated the options the respondents had to choose from.

Question	Option 1	Option 2	Option 3	Option 4	Option 5
Q2.2	While Studying	Websites/ Newspaper	From Friends	Other	
	19	10	1	4	

Q2.3	6	7	8	9	10
	12	1	25	2	5
Q2.4	Lowercase	Uppercase	Combination		
	0	0	45		
Q2.6	Every 90 days	Every120 days	Never	Don't know	
	38	4	1	2	

Table 4: Theoretical questions results (n=45)

As can be seen in Table 4, Q2.2, 19 (42%) respondents stated they received password guidance whilst studying and 10 (22%) respondents stated receiving password guidance from websites or newspapers. For Q2.3, 25 (55%) respondents indicated that the minimum number of characters is 8, 12 (26%) respondents indicated a minimum of 6 characters. For Q2.4, 100% of the respondents indicated that a password should contain a combination of uppercase and lowercase characters. For Q2.6, 38 (84%) respondents answered that users should change their passwords every 90 days.

For the open-ended question, Q2.9, 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.

5.3. Actual password behaviour

This section discusses the results and findings relating to the actual password behaviour of students. Table 5 lists the questions which were asked using a 5-point Likert Scale where 1 = '*always*', 3 = '*sometimes*' and 5 = '*never*'. Those questions not using this scale are omitted from this table but are discussed in this section.

In Table 5, the numbers in brackets are calculated as follows – the number of respondents is multiplied by the Likert Scale option number. For example, 11 respondents chose option 2 for Q3.1. Therefore, the number in brackets is 11x2 = 22. All the numbers in brackets are then added together for the Total. The Average is calculated by dividing the Total by the number of respondents (n=45).

Questions	Scale					Tot	Avg
	1	2	3	4	5		
Q 3.1	13 (13)	11 (22)	11 (33)	7(28)	3 (15)	111	2.47
Q 3.2	4 (4)	4 (8)	7 (21)	7(28)	23 (115)	176	3.91
Q 3.3	12 (12)	10 (20)	10 (30)	4(16)	9 (45)	123	2.73
Q 3.6	4 (4)	5 (10)	8 (24)	5(20)	23 (115)	173	3.84
Q 3.7	1 (1)	3 (6)	5 (15)	3 (12)	33 (165)	199	4.42
Q 3.15	1 (1)	3 (6)	7 (21)	9 (36)	25 (125)	189	4.2

Table 5: Likert scale questions (n=45)

Table 5 depicts the average for the questions which made use of a 5-point Likert Scale. Those questions with an average of 4.0 or higher, indicate good password behaviour, whereas those with an average of less than 3.0 indicate fairly poor behaviour. From this it can be argued that the respondents behave best when it comes to never using dictionary words as passwords and they generally use stronger passwords to protect those accounts which require extra protection.

For Q3.1, 13 (28%) respondents stated they *'always'* reuse their password whereas 3 (6%) respondents stated they *'never'* reuse their passwords. For Q3.2, 23 (51%) respondents said their passwords were '*never'* plaintext only, whereas 4 (8%) respondents' passwords are '*always'* plaintext. For Q3.3, 12 (26%) respondents stated that their passwords were '*always'* less than 10 characters, 10 (22%) respondents indicated *'sometimes'* and a further 10 (22%) stated their passwords are '*sometimes'* less than 10 characters. For Q3.6, 23 (51%) respondents stated that they '*never'* use personal dates and family member names as passwords. For Q3.7, 33 (73%) respondents said they '*never'* use dictionary words as passwords, and for Q3.15, 25 (55%) respondents stated that they *'never'* use their regular password in the accounts they think should be extra protected.

For Q3.4, 40 (89%) respondents have used the same password for multiple accounts. Similarly, for Q3.5, 40 (89%) 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 Q3.8, 14 (31%) respondents indicated that they change their passwords every 120 days and 7 (16%) participants do not change their passwords at all. For Q3.8, 6 (13%) respondents actually change their passwords every 90 days. For Q3.12, 39 (87%) respondents do not share passwords. For Q3.14, 17 (37%) respondents do not delete their online accounts if they have not used them in a long time.

6. Discussion

This section discusses the results and findings from the survey by comparing the theoretical password knowledge with the actual password behaviour. There are a number of theoretical password knowledge questions, as were seen in Table 1, which can be correlated to the actual password behaviour questions, as seen in Table 2. Table 6 lists the theoretical and behaviour-related questions that can be correlated.

Characteristic	Theoretical Password Knowledge Questions	Actual Password Behaviour Questions
Minimum password length	Q2.3	Q3.3
Password characteristics	Q2.4	Q3.2
Changing passwords	Q2.6	Q3.8
Delete online accounts	Q2.7	Q3.14
Writing passwords down	Q2.8	Q3.10

Table 6: Correlation between theoretical password knowledge and actual password behaviour questions

Figure 1 represents the respondents' theoretical password knowledge compared to their actual password management behaviour. For these results, only the top most answered questions are represented. For example, Q2.3, 25 (56%) of the respondents indicated that the minimum password length should be 8 characters, whereas in Q3.3 only 9 (20%) of the respondents indicated that their passwords are '*always'* less than 10 characters.

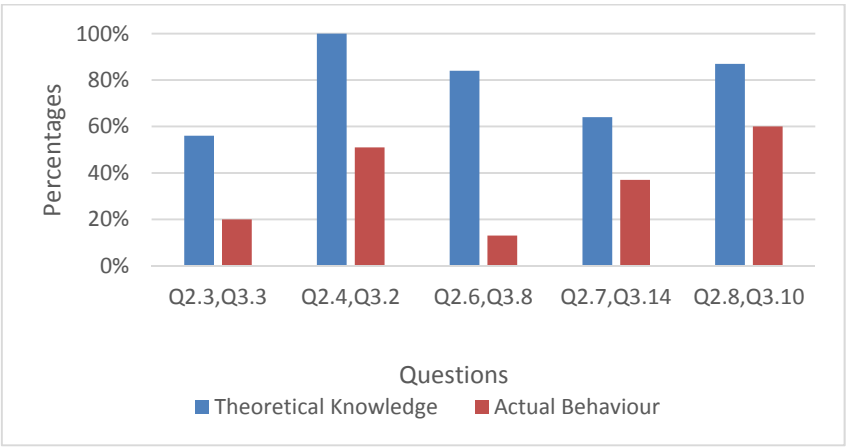

Figure 1: Theoretical knowledge versus actual behaviour

As can be seen in Figure 1, there is a difference between the respondents' theoretical password knowledge and their actual password behaviour. In Q2.3 and Q3.3, which referred to the minimum password length, it can be seen that the respondents know

what the minimum average length should be for a password but when it comes to actually putting it into practice they are not adhering to it. Q2.4 and Q3.2, which referred to the password characteristics, show that the users are aware of the fact that a password should contain a combination of uppercase and lowercase characters. However, when it comes to the actual behaviour, only 23 (51%) of the respondents put the theory into practice by stating they '*never*' use passwords which are plaintext. In Q2.6 and Q3.8 which referred to how often passwords should be changed, 38 (84%) of the respondents indicated that they know how often to change their passwords, but do not use this knowledge in practice. In Q2.7 and Q3.14, which referred to the deleting of online accounts, it can be seen that the respondents know that online accounts should be deleted if they are not using it, but are not using this theoretical knowledge in practice. Lastly, Q2.8 and Q3.10, which referred to writing passwords down, show that respondents are aware that they should not write their passwords down, however, with regards to their actual behaviour there is still a large number of people who write passwords down on text files and sticky notes.

7. Conclusion

As discussed, it is very important that people understand the importance of passwords and password management. Based on the theoretical password knowledge results and findings from the survey conducted, it can be seen that these respondents are educated on good password management and have the necessary theoretical knowledge. However, from the actual password behaviour results and findings, it can be seen that there is a difference between the respondents' knowledge and their actual behaviour. By not applying the theoretical password knowledge in practice, it can be argued that users are exposing themselves to risk. This research was limited in that it focused on IT students and the results are not to be generalised. Further research is required to understand this identified gap between users' password knowledge and behaviour. It could be argued that good password behaviour is more likely to be demonstrated by those users who have experienced the consequences of poor password behaviour, thereby re-enforcing the importance of good password management.

8. Acknowledgements

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

9. References

Apple (2013).OS X Mountain Lion: Tips for creating secure passwords. Apple.[online] Available at: https://support.apple.com/kb/PH10624?locale=en_US [Accessed 26 April. 2015]

Apple (2016). Security and your apple ID. Apple.[online] Available at: https://support.apple.com/en-za/HT201303 [Accessed 8 March.2016]

Blanchard.J. (2014). Weak passwords put millions at risk of bank accounts and other information being hacked online. Mirror.[online] Available at: http://www.mirror.co.uk/news/technology-science/technology/weak-passwords-put-millions-risk-4439460 [Accessed 25 March.2015]

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P.C. and Biddle, R., 2009, November. Multiple password interference in text passwords and click-based graphical passwords. *In Proceedings of the 16th ACM conference on Computer and communications security* (pp. 500-511). ACM.

Gaw, S. and 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.

Google (2016).Name and password guidelines. Google.[online] Available at: https://support.google.com/a/answer/33386?hl=en [Accessed 8 March.2016]

Helkala, K., 2011. Password education based on guidelines tailored to different password categories. *Journal of Computers*, *6*(5), pp.969-975.

Helkala, K. and Hoddø Bakås, T., 2014. Extended results of Norwegian password security survey. *Information Management & Computer Security*,*22*(4), pp.346-357.

Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F. and Lopez, J., 2012, May. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. *In Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 523-537). IEEE.

Li, Z., He, W., Akhawe, D. and Song, D., 2014. The emperor's new password manager: Security analysis of web-based password managers. *In 23rd USENIX Security Symposium (USENIX Security 14)* (pp. 465-479).

McDowell, M., Hernan.S & Rafail.J. (2013). Security Tip(ST04-002): Choosing and Protecting Passwords. US-CERT.[online] Available at: https://www.us-cert.gov/ncas/tips/ST04-002 [Accessed 25 March. 2015]

Microsoft (2012). Maximum password age. Microsoft.[online] Available at:https://technet.microsoft.com/en-us/library/hh994573(v=ws.10).aspx [Accessed 27 April.2015]

Microsoft.(2015).Tips for creating a strong password. Microsft.[online] Available at: http://windows.microsoft.com/en-za/windows-vista/tips-for-creating-a-strong-password [Accessed 25 April,2015]

Renaud, K., Mayer, P., Volkamer, M. and Maguire, J., 2013, September. Are graphical authentication mechanisms as strong as passwords?. *In Computer Science and Information Systems* (FedCSIS), 2013 Federated Conference on (pp. 837-844). IEEE.

Schofield, J. (2013). Hotmail are my lost accounts a security risk.The Guardian.[online] Available at: http://www.theguardian.com/technology/askjack/2013/jul/18/hotmail-lost-accounts-security-risk [Accessed 15 June. 2015]

Stobert, E. and Biddle, R., 2014. The password life cycle: user behaviour in managing passwords. *In Symposium On Usable Privacy and Security (SOUPS 2014)* (pp. 243-

255).http://www.theguardian.com/technology/askjack/2013/jul/18/hotmail-lost-accounts-security-risk

TeamsID (2016). Worst Passwords Of 2015.[online] Available at: https://www.teamsid.com/worst-passwords-2015/ [Accessed 10 March. 2016]

University of Illinois (2014). Why you should use different passwords. University of Illinois.[online] Available at: https://security.illinois.edu/content/why-you-should-use-different-passwords [Accessed 30 April,2015]

Weir, M., Aggarwal, S., Collins, M. and Stern, H., 2010, October. Testing metrics for password creation policies by attacking large sets of revealed passwords. *In Proceedings of the 17th ACM conference on Computer and communications security* (pp. 162-175). ACM.