ESI Preprints **Not Peer-reviewed**

How Students Deal With Password Security: Case Study of Nalut University Students

Al -Jerbie Saida Issa
Jernaz Riad Suliman
Askar Ekram
Benhamed Doa
Kamis Zahra
OunAllah Salsabill
Faculty of education/ Nalut, Nalut University, Libya
Computer Department

Doi: 10.19044/esipreprint.4.2024.p505

Approved: 15 April 2024
Posted: 18 April 2024

Cite As:
Al -Jerbie S.A., Jernaz R.S., Askar E., Benhamed D., Kamis Z. & OunAllah S. (2024). *How Students Deal With Password Security: Case Study of Nalut University Students*. ESI Preprints. https://doi.org/10.19044/esipreprint.4.2024.p505

Abstract

University students are the largest segment of society that uses modern technology, represented by computers and smart phones, and to ensure the security and integrity of information, students must consider the most common protection methods for conducting the electronic authentication process. This research seeks to evaluate the extent of awareness of Nalut University students about password policies. The size of the study sample was (539) students, and the average age of the sample was (between 18 and 20 years) out of 2177 students. The questionnaire was analyzed using the statistical analysis program SPSS, version (26). The results of the study showed that the level of awareness among Nalut University students was low, as their percentage was 49.8%. It was found that there is a relationship between gender and password policy among university students, where the p value was = 0.01.

Keywords: Password, password security, security risks, university students

1. Introduction

The global technological escalation and scientific dependence on the use of digital technology in various scientific and entertainment fields has become a feature of the modern era, and developing countries have a share of this scientific and technological progress that has become apparent in many fields. The most prominent of these is the inclusion of computers and smart phones in the fields of learning, scientific research and entertainment, as developing countries are truly working to keep pace with development and modernity on an ongoing basis among many institutions of higher education based on the reliance on the use of technology, which has resulted in the need to work to secure the information that People deal with it to prevent loss of necessary data, and the ability to control information and harness it to serve the scientific and research reality in universities (Bashaer, 2019).

The Internet is a wide field and an integrated system, where many users communicate with each other, but in this system, passwords are the security key for all the user's personal details, as users can use the Internet in many electronic operations and transactions, and this requires entering many personal details. In order to provide a higher level of security, passwords must be taken care of in terms of making them easy for the user to remember, and difficult for others to guess (Vankadesh & Palanivel, 2015) Florêncio, 2010), (seitz et al., 2017).

The most prominent and most widely used methods for evaluating password security are the evaluation index provided by the National Institute of Standards and Technology (NIST), which analyzes the complexity of passwords according to combinations of upper- and lower-case letters, numbers, and special symbols, in addition to the zxcvbn evaluation index, which evaluates security by rating a list with passwords that common users employ frequently and randomly (Carnavalet & Mannan, 2015).

Passwords are one of the most common methods for controlling user authentication and providing easy access to user system information Quermann, Harbach & Dumuth 2018). Given the widespread reliance on the use of passwords in daily life (Wiefling et al.,2022) , very little attention has been focused on the properties of passwords in terms of (configuring, saving, resetting them). Using them, as passwords that are difficult to remember, they are also complex in their composition, and this would increase the chances of writing them down to retrieve them, as a result, students could be a victim of the attackers (Mazurek et al., 2013), (Dell'Amico, 2010), Florêncio & Herley 2007) . Malone & maher, 2012)

The main aspect of this study was to assess the level of password security awareness among university students (Nalut university) and to present the best recommendation from our findings to ensure reliable implementations for good password security practices.

2. Related work

Students' risky behaviors when dealing with passwords, then verified in a number of studies. A number of studies focused on studies of students' behaviors in managing passwords, in terms of ways to create and store them, and how to share them with others. as any user, the students tried to deal with the problem of hacking passwords in several ways, including using password management programs, in addition to other risks, such as accessing their accounts via free Wi-Fi or any available hotspot. The next part briefly reviews some of these paragraphs.

Mazurek et al., (2013) studied the single-sin on passwords used by over 25,000 faculty, staff, and students of Carnegie Mellon University (CMU). The collected passwords were analyzed by the password cracking algorithm in order to obtain the risks in the case of off-line attack. A significant finding of this study indicated that students of computer science school make passwords more than 1.8 times as strong as those in the business school. Furthermore, user who complying with university policy have weaker passwords with 46% more likely to be guessed. When users who use numbers for some of the letters in a word or name 54% are likely to be guessed. Adams & Sasse (1999) conducted a study on user behaviors related to passwords, including password creation, reuse, recall, work practices, and summarized that participants lacked security motivation, understanding of password policies, and tended to circumvent password restrictions for convenience.

Brown et al., (2004) clarified in a survey study involving 218 university students at Southern Methodist University to assess and establish students' password practices and usage behavior. The survey showed that students have an 8.18% password reuse rate with 4.45% using different passwords for these functions. The average password strength is 1.84%. Two-thirds of the passwords are designed around personal traits, while the rest are mostly related to accounts of relatives and friends that require a password, with only 4.45% having a password. The majority of participants (92.9%) reused their passwords in at least one account. Gaw& felten) 2006) focused on understanding password management behavior among students. The first study relied on a laboratory study, users were asked to log in to various websites to accurately assess the number of passwords they use and reuse. Forty-nine American university students participated in the study, and it was found that the majority of students have three or fewer passwords, and they tend to reuse these passwords. The second study focused on the reasons for password reuse, where a questionnaire was distributed to 58 university students from the same sample as the first study. The results showed that the majority of respondents (60%) reused passwords for ease of remembering them, while other responses (14%) indicated having multiple accounts.

In a study conducted by Notoatmodjo & thomborson et al., (2009) at a university in New Zealand, the study sample consisted of (26) students. The study focused on the students' ability to classify their online accounts appropriately in terms of importance, with online banking accounts classified as highly important accounts, while newspaper accounts were classified as accounts of low importance. The results showed that the more online accounts students had, the higher the likelihood of password reuse. Although they reported avoiding reusing passwords for high-importance accounts, (35%) of students reported reusing passwords because they are easy to remember, while (19%) reported reusing passwords for accounts of similar value. Additionally, (18.5%) reported reusing passwords for similar accounts.

In a study conducted by Wash et al., (2016) they focused on collecting data on the password activities of a sample of 134 university students. The study linked self-reporting behavior with real-world behavior to highlight the human aspect of security credibility. The results showed that the average number of passwords for students is around 12 different passwords, and the average number of online logins is 17.5 accounts, indicating the reuse of some passwords. Furthermore, additional analyses revealed the removal of login attempts containing password typos. Additionally, reusing a strong password puts users at risk of having multiple accounts stolen if guessed. Szasz & Kiss (2018) clarified in a study conducted on students at Obuda University, the study aimed to test the effectiveness of cyber training programs and evaluate and develop educational methods. In this study, students were divided into two groups and their results were compared. In the first group, students watched an explanatory video on decrypting passwords using programs, while the second group was given the authority to choose these programs. The study relied on using an electronic questionnaire to measure their secure and risky behaviors before and after the training program by examining their use of passwords and devices. The study results indicated that the first group did not show any significant changes in their behaviors, while the second group showed substantial changes in their user behavior in terms of password length, password composition, number of password changes, and use of protected points and Wi-Fi, reaching 52.6%, which highlights the importance of training programs in increasing security awareness among students. Taneski et al.,)2019 (In a systematic review of 82 studies published between 1978 and 2018 on password security issues, it was found that password reuse was the most common problem.

Ur et al., (2015) conducted a laboratory study in which participants created three passwords under different password policy conditions. Three participants out of 49 (6%) used the same password in all cases, 10 (20%)

used the same password in two out of the three cases, while 10 other participants reused a password with some variations, often very simple. Previous studies have documented factors that lead to password guessing ease, but have not identified the reasons why users formulate weak passwords. Participants reported that using birth dates or names is secure if a special character is added at the end. Only 3% of participants reported not reusing the same password, despite the majority stating that they use secure algorithms to create passwords.

Looking at the risky password management behavior of users, it became clear that using, recording, and sharing passwords with others is one of the main risks. Although most password management systems alert users to risky behavior that could expose passwords to others, such as logging into accounts from shared computers or from a friend's or colleague's device, many users still do not pay attention to these guidelines and act in ways that put them at risk of being hacked, as shown in previous studies. In addition, to ensure the best way to collect the data from the mentioned participants a quantitative methodology conducted by using a questioner as presented in the related word from the previous studies.

3. Methods

This study was conducted using both (online and offline) questionnaire. The online questionnaire was implemented via Google forms. The designed questionnaire divided into three sections. The first section presented the demographic information, the second section focuses on assessing passwords security practices, and finally the third section measuring the behavior of students regarding to password security.

4. Study Hypotheses

- There is a relationship between gender and password security.
- There is no relationship between creating passwords and how they (memorized stored) and its importance

5. Results

The data set includes 500 students who completed the questionnaire.

In the first section we precent the demographic information collected from the chosen sample, it was found that 26.7% (144) were male and 73.3% (395) were female. In term of the academic year, the sample size was distributed as follow, 30.4% were in the first year, 25.6% were in the second year, 20.4% were in the third year, and finally 23.6% were in the fourth year. In order to identify the different faculties in Nalut University the results represent that 19.2% were from faculty of education, 41.6% faculty if medical technology, 12.8% faculty of law (Nalut), 15.2% faculty of

Economic and Political science, 7.1% faculty of Engineering (Gadu), 2.2% faculty of Science and Arts (Gadames), finally 1.9% to the Faculty of Law (Al-Rahibat).

The second section was asked students how they dealing with password security, the results declared in a high percentage 37.7% that they changing their passwords in a case of facing a security attack, while 29.5% never change their passwords, 17.3% change it once or less in a year, while 9.5% every (3 to 6) a month, and in a low percentage 6.1% change it (1 to 2) months. The number of passwords deployed by students varied as they indicated, were 64% have (1-3)passwords, 19.1% have (4-6) passwords, finally 16.9% have seven or more passwords for every electronic device.

In contrast, students tent to have different practices in number of passwords used for every e-mail and social mail, as 19.5% never use different passwords for each e-mail or social mail, 19.3% rarely, as a result these negative indication lead students to face the risk of being hacked by attackers. On the other hand, 23.9% sometimes, 14.1% students they often change their passwords, and the 23.2% precents a slight level of awareness were answered by (always) have different passwords for every e-mail and social mail. Another risk discussed with students when we asked them were if sharing their passwords via internet, students showed a high level of awareness as they scored 83.3% never share their passwords, 8.7% rarely share it, while 4.5% answered with sometimes, 2% usually, and only 1.5% present low level of awareness when always share their passwords via internet.

Forgetting passwords is the main threats that students faced while attempting to access to their e-mails or devices, as it results in facing blocks after several attempts. In general, 61.5% answered with never and 16,9% rarely face any blocks after multiple attempting of resetting passwords in short period of time, which could be referred to the type and number off passwords they have. The students answer about using same password for another system, it was found that 27.7% never use the same passwords and 15.8% rarely dose so as showed in table 1.

Table 1. Students security practices with passwords

Using Wi-Fi – sharing point			
In every chance	In case of secured points	never	
70.3%	21.2%	8.5%	
share your passwords			
With close friend	Member of the family	With any one	Never share my password
30.4%	42.1%	4.3%	23.2%
Forget important password			
One time	Two times	Many times	never
31.4%	11.5%	53.6%	3.5%

Number of passwords used in electronic devices				
(1-3) passwords		(4-6) passwords		Seven or more
64%		19.1%		16.9%
Different passwords for every e-mail- or social mail				
Never	Rare	Sometimes	Usually	Always
19.5%	19.3%	23.9%	14.1%	23.2%
Sharing passwords via internet				
Never	Rare	sometimes	Usually	Always
83.3%	8.7%	4.5%	2%	1.5%
Facing blocks after many reset attempts				
Never	Rare	sometimes	Usually	Always
61.5%	16.9%	14.7%	4.5%	2.4%
Using same password for another systems				
Never	Rare	sometimes	Usually	Always
27.7%	15.8%	28.6%	16%	11.9%

The second section presents the students security behavior according to passwords as shown in table 2:

Table 2. Students behavior award password security practices

Using complex passwords				
Small letters	Numbers only	Capital and small letters, and numbers	Capital and small letters, numbers, special characters	
12.4%	18.6%	38%	31%	
Ways of saving passwords				
Allow browse to store the password	Write all password	Save important passwords	Save password in my memory	Use Password manage-ment programs
25.8%	18%	12.6%	38.6%	5%
Password contains personal information (ID- date of birth..etc.)				
Never	Rare	Sometimes	usually	Always
38.6%	11.7%	25%	14.5%	10.2%
Facing difficulties in remembering passwords				
Never	Rare	Sometimes	usually	Always
17.7%	17.3%	35.8%	12.1%	17.1%
Changed your password because you felt it might have been guessed/hacked?				
Never	Rare	Sometimes	usually	Always
25.4%	18.5%	27.5%	17.1%	11.5%

From the previous results we found that the level of passwords security awareness was slightly high as it scored (49.8 %) from the positives feedbacks, which presents the need to educate students about the standards of creating passwords. Password creations is the first stage of defense against

the attackers, as when we asked students about the contains of their passwords, 12.4% use lower-case letters only, 18.6% use numbers only, 38% use lower and upper-case letter with numbers, and finally 31% use all the previous cases with special characters. Furthermore, the way of storing passwords presents another way of threats, were 25.8% allow the browser to store their password, 18% write done all passwords, 12.6% save only the important passwords, while 5% uses password management programs, and only, 38.6% memories their passwords which could be referred to the contain of the password which make it easy to remember.

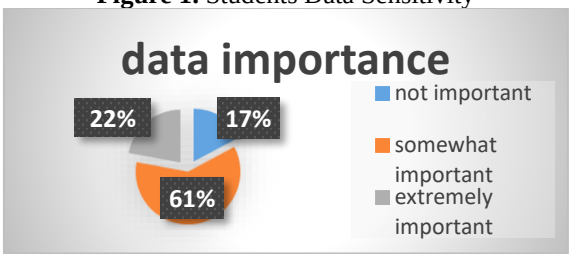
As a formal user, we asked students about the contain of their passwords (ID- Date of Birth…), 38.6% students declared they never dose so, 11.7% rarely, 25% sometimes, 14.5% usually, and around 10% always use related personal information in their passwords. Furthermore, students' answers diverged on facing difficulties in remembering passwords, were 17.7% never have any difficulties, 17.3% rarely, 35.8% sometimes, 12.1% usually, and finally 17.1% always dose so.

Although there was a slight level of awareness with 37.7% (203, students) change their password in case they hacked, 29.5% (159) never change their passwords, and around (17.3% - 6.1%) change their passwords between (two to three months) and (three to six) months. This finding comes into agreement with the study of (Zaviran & Haga, 1999) and (Ur et al.,2015). This could be referred to the data sensitivity that protected using strong passwords. As a highly sensitive data enforce students to provide high level of security protection and as a result, change their passwords regularly.

6. Discussion

To stand on the students' awareness on how they classify their information importance, they tend to have a slit level of awareness as they stated in the figure 1.

Figure 1. Students Data Sensitivity



These results attributed to the importance of data protected via passwords. High important data makes it vulnerable to attackers, which enforce students to change their passwords. On the other hand, low importance data makes it less vulnerable to be hacked, as a result students

overlook change their passwords periodically. This aligns with a study by Notoatmodjom (2009), where 35% of students reported avoiding reusing passwords for high important accounts.

A null hypothesis of there is a relationship between gender and security practices of the passwords (using Wi-Fi-Hotspots- creating- storing -remembering -changing) passwords, was accepted with the value of 0.010 in case of using (wifi-hot spots) which refers to strong relationship between it. Furthermore, a relationship between gender and some passwords practices with the value less than 0.05 which comes to agreement (Bonneau,2012) and (Michelle et al., 2013). And conflicts with (Merdenyan & Petrie, 2022). The finding of correlation between the strength of the password and study variable was convergence with the value (0.014) in case of data sensitivity where students' high data value has more strong and complex passwords consisting numbers, letters, and symbols which provide high level of protection. in construct, it is conflicting with creating and remembering passwords with the value (0.999-0.628), these finding confirm (Zviran & Haga. 1999) in data sensitivity.

Conclusion

The digital authentication enforce student to access their information with a high level of security, to prevent any potential treats, loss, and attacks to their information. This study aimed to assess the level of passwords security awareness. The result shown that students appears an acceptable level of awareness in some of security practices re- grading password security, furthermore student behavior percent many vulnerabilities which results in losing their information in any possible attacks. A future recommendation should focus in applying more studies for greater sample size since the researcher cannot reach a lot of respondents due to spatial distance of university faculties. Lastly, the recommendation to conduct a security training program to ensure a real improvement in student password security awareness.

Conflict of Interest: The authors reported no conflict of interest.

Data Availability: All data are included in the content of the paper.

Funding Statement: The authors did not obtain any funding for this research.

References:

1. Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46.

2. Bashear, E.A. 2019. The Degree of Using Smartphones by Jordanian Private Universities Students in Teaching on Quality Criteria. MIDDLE EAST UNIVERSITY. Master Thesis.
3. Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition*, *18*(6), 641-651.
4. Carnavalet, X. D. C. D., & Mannan, M. (2015). A large-scale evaluation of high-impact password strength meters. ACM Transactions on Information and System Security (TISSEC), 18(1), 1-32.
5. Dell'Amico, M., Michiardi, P., & Roudier, Y. (2010, March). Password strength: An empirical analysis. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). IEEE.
6. Florêncio, D., & Herley, C. (2010, July). Where do security policies come from?. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (pp. 1-14).
7. 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).
8. 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).)
9. Mazurek, M. L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., ... & Ur, B. (2013, November). Measuring password guess ability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 173-186).
10. 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).
11. Notoatmodjo, G., & Thomborson, C. D. (2009, January). Passwords and Perceptions. In AISC (Vol. 9, pp. 71-78).
12. Quermann, N., Harbach, M., & Dürmuth, M. (2018). The state of user authentication in the wild. *WAY*, *18*.
13. Seitz, T., Hartmann, M., Pfab, J., & Souque, S. (2017, May). Do differences in password policies prevent password reuse?. In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (pp. 2056-2063).
14. Szasz, A., & Kiss, G. (2018). Multimedia password retrieval programs in information security education. JOURNAL OF APPLIED MULTIMEDIA, 13(3), 87-96.

15. Taneski, V., Heričko, M., & Brumen, B. (2019). Systematic overview of password security problems. Acta Polytechnica Hungarica, 16(3), 143-165.
16. Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., ... & 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).
17. Venkadesh, S., & Palanivel, K. (2015). A survey on password stealing attacks and its protecting mechanism. *International Journal of Engineering Trends and Technology (IJETT)*, *19*(4).
18. Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (pp. 175-188).
19. Wiefling, S., Jørgensen, P. R., Thunem, S., & Iacono, L. L. (2022). Pump up password security! Evaluating and enhancing risk-based authentication on a real-world large-scale online service. *ACM Transactions on Privacy and Security*, *26*(1), 1-36.
20. Zviran, M., & Haga, W. J. (1999). Password security: an empirical study. *Journal of Management Information Systems*, *15*(4), 161-185.