DOI: 10.21917/ijsc.2025.0557

CRACKS IN DIGITAL DEFENSE: A STUDY ON PASSWORD SECURITY AWARENESS AND BEHAVIOR IN COLLEGE STUDENTS

Subitha Sivakumar[1] and Sivakumar Venkataraman[2]
[1]*New Era College of Arts, Science and Technology, Botswana*
[2]*Botho University, Botswana*

Abstract

In the digital age, password security is an important part of cybersecurity, especially for university students who often access online platforms for academic and personal use. This study examines the perceptions and perceptions of password security under university students, and examines knowledge, practices, and attitudes to protect online accounts from Botswana. Research uses a survey based on a survey to assess the understanding of students strongly creating passwords, using multi-factor verification and their vulnerability to cyber threats such as phishing and theft of credentials. The findings reveal a significant abyss between consciousness and implementation, with many students acknowledging the importance of password security, but do not take robust protective measures. Furthermore, in this study, Password security practices are highlighted, including comfort, lack of cybersecurity and low risk of cyberattacks. This research emphasizes the need for an increased campaign for education and awareness of cyber security within academic institutions to bridge the abyss between knowledge and practice. The study recommends integrating password security training in the curriculum, to promote the importance of password management and encourage the students to follow the rules and procedures for regular passwords change and multi-factor verification. By strengthening the awareness of password security with students is essential to improve cybernetic risks and ensure the protection of personal and institutional data.

Keywords:

Password Security, Cybersecurity Awareness, College Students, Online Safety, Authentication Practices

1. INTRODUCTION

In today's interconnected world, the security of the online account has become a growing problem, especially for students who often approach digital platforms for academic, social and financial activities.

Looking at the growth of online service usage, it shows the importance of preventing strong password protection in contradiction of unauthorized access. Although the usage of technology worldwide, many students are sensitive to cyberthreats, due to that the students don't take helpful measures to ensure password security [10].

While many students recognize the importance of secure slogans, there is often a gap between consciousness and real practice. Risk behavior, such as the reuse of passwords in some accounts, selecting weak or predictable passwords, and neglecting multi-factor authentication contributes to safety gaps. These habits are often based on underestimating comfort, lack of education in the field of cyber security and poor risk management.

Examination of these factors is to emphasize the importance of strengthening security procedures in academic institutions. Support for implementation of proven procedures such as Use of password manager and implementation of stricter verification methods can help reduce risk and improve digital security. The findings of this study provide valuable insights into the behavior and challenges related to the security of slogans among university students, preparing a way for targeted sensitization initiatives and improving cyber security instructions.

The objective for the study,

- To find if the students have passwords or authentication security for android devices and other online accounts.
- To analyze the students' perceptions of password security and the effectiveness of protecting the devices.
- To determine the students are using the best practices in creating passwords such as in avoiding their personal information and avoiding the character diversity, and to determine how often students change their passwords.
- To Determine whether students use the same password for multiple accounts.
- To find out how students maintain their passwords.

2. LITERATURE REVIEW

In cyber security, password security remains an important concern in the development of digital security platforms that affect the academic and personal domain in universities students. Online platforms are mostly used by the students, so it's important to understand the user behavior and the understanding of password management among students.

Researchers have conducted many studies in password management among students. According to [2] from the study found that the students have the basic knowledge on security measures like to have strong passwords, but even though failed to implement them effectively. This shows the disconnect between hypothetical knowledge and actual behaviors on real time trend in reusing passwords, creating a weak password and rarely updating the passwords.

Similarly, [7], [19] stated an experimental analysis of reusage and updating the passwords. The research findings provided a general tendency among users to reuse passwords within several online platforms, some with an insignificant variation, making highly susceptible to credential cyber-attacks. This type of behavior is widespread between students aged from 18 to 25, a demographic that overlaps heavily with college students.

Password composition is also a concern among students and should be considered as a weak zone. In technical, [16] research focused on the information technology students on about password management and found that the students have better knowledge on password management, even occasionally resorted to insecure behaviors for the sake of convenience. This study

indicates the need for practical training, not theoretical understanding in cybersecurity.

The concern of including personal information in password creation studied by [8] proved the users incorporate their personal details while creating the passwords. This pattern makes it easy to predict and cracked by the hackers. Even though dated, this finding still reminds relevant as similar behaviors continue among university students.

A recent analysis from [20] focused on password management skills and found that the students had low adoption of password managers tools. Even though with the availability of password security techniques, most students are used to memorizing their passwords or note down somewhere without encryption. This leads to a significant risk where the password is exposed to friends or in the living areas.

3. METHODOLOGY

For this study, the survey-based methodology was used as an online questionnaire to evaluate the password security awareness and practices among college students in Botswana. This questionnaire includes both demographic information and questions related to password security to help us to understand how the students are managing the passwords.

3.1 DEMOGRAPHIC DETAILS

- Gender
- Age Group: Below 15, 15-16, 17-18, 19-20, Above 20
- Degree Registered: Certificate, Diploma, Under-graduate, post-graduate
- Field of Study: Whether it is relevant to computer science
- Computer Knowledge and Skills: Self-assessed level of proficiency
- Internet Access: Availability of internet at home
- Smart Devices: Ownership and number of Android (Smart) devices

3.2 PASSWORD SECURITY PRACTICES AND PERCEPTIONS

- Device Protection: Use of passwords on all personal devices
- Password Strength: Perception of password security for devices
- Password Composition: Whether passwords have at least 10 characters with a mix of alphabets, numbers, and symbols

3.3 PASSWORD MANAGEMENT

- Frequency of password changes
- Use of personal information (name, date of birth, etc.) in passwords
- Reuse of passwords across multiple websites and services
- Methods for storing passwords (memorization, writing down, saving in devices)
- Whether passwords have been shared with family or friends
- Encryption of stored passwords if saved in any format

3.4 PARTICIPATION DETAILS

The student participation was classified based on the following demographic components,

- Gender: Female, Male and Prefer not to say
- Age Group: 15 and below, age group 16-17, age group 18-19, age group 20 and above
- Course registered: Certificate, Diploma, Under-Graduate, Post-Graduate

4. DATA COLLECTION

For this study, the online questionnaire is designed to determine the knowledge, practices and perception in terms of password security among the college students. These questionnaires include multiple choice to assess the level of awareness and the security habits of students in managing their passwords. This survey was distributed across various colleges in Botswana and a total of 167 students were participated. The data were collected and used to find the trends and differences among students across demographics and potential areas for improving password security awareness among college students in Botswana.

5. RESULT ANALYSIS

This analysis represents the findings of the study on the awareness and perception of the password security within the college students in Botswana. The data collected from 167 students are examined to find the trends, patterns and key insights related to students understanding and practices regarding password security. This section presents a thorough analysis of the survey results, emphasizing important areas that need focus to improve college students' password security habits.

The Table.1 shows that 167 college students are surveyed in Gaborone, Botswana were female (101) students with high representation when compared to male (56) respondents with five participants preferred to not disclose their gender and five responses are missing. Table.1 shows how the participants are distributed in age, where the 19-20 age group with 77 students has the most participants, followed by 20 years and above age group with 66 students. A small number of students of 17-18 age group with 19 students and followed with two students in the age group of 15-16.

Table.1. Demographic Analysis

(a) Gender

Gender		Prefer not to say	Missing Values
Male	Female		
56	101	5	5

(b) Age Group

< 15	15-16	17- 18	19– 20	> 20	Missing Values
0	2	19	77	66	3

5.1 ACADEMIC BACKGROUND AND COMPUTER KNOWLEDGE ANALYSIS

Most participants in the study were undergraduate students (121), followed by postgraduate students (26) and diploma students (10). Only two students were enrolled in certificate programs, while eight responses were missing. This distribution indicates that most respondents were pursuing higher education at the undergraduate or postgraduate level, which may influence their exposure to digital security practices.

Table.2. Academic Background and Computer Knowledge Analysis

Course Registered				
Certificate	**Diploma**	**Under Graduate**	**Post Graduate**	**Missing Values**
2	10	121	26	8
Level of computer knowledge and skill				
Beginner	**Intermediate**	**Expert**	**No Experience**	**Missing Values**
65	93	7	0	2

Regarding computer knowledge and skills, most students rated themselves as having intermediate proficiency (93 students), while 65 students identified as beginners. A small proportion of respondents (7 students) considered themselves experts, and none reported having no computer experience. However, two responses were missing. This data suggests that while most students have some level of computer proficiency, a significant number still have only basic knowledge, which could impact their awareness and adoption of password security practices.

- **Objective 1**: To find if the students have passwords or authentication security for the android devices and other online accounts.

The Table.3 shows that most of the students have at least one Android devices with 78 participants, followed with 47 students having two android devices. Only a small number reported having three android devices with 27 participants, followed by 4 participants with four or more participants. Notably, five students did not own any smart devices, and six responses were missing. This shows that high numbers of participants are having android devices which shows the importance of secure password management.

When asked about password usage on their devices, 131 students confirmed using passwords, while 35 students did not, and one response was missing. This shows that majority of the participants recognized the importance of password protection, where the significant number of participants with 35 don't use password protection raises a big concern, and shows that a lack of awareness in digital safety practices.

Table.3. Device Protection

Password used in Devices		
Yes	**No**	**Missing Value**
131	35	1

Number of Android (Smart) devices					
0	**1**	**2**	**3**	**4 and above**	**Missing Value**
5	78	47	27	4	6

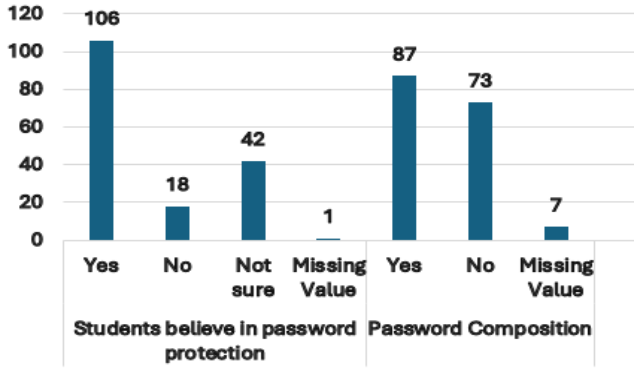

Fig.2. Password Strength

- **Objective 2**: To analyze the students' perceptions of password security and the effectiveness of protecting the devices.

Table.4 shows that the students with 106 agreed password protects their android devices, indicating confidence in password security. But the fear is that 19 students did not agree to believe the password protects their android devices, and 42 students were uncertain about password security. That suggests that a significant portion of respondents may lack awareness or trust in the effectiveness of password security. One response was missing.

Regarding password composition, 87 students agreed that using passwords that meet security standards (i.e., at least 10 characters with a mix of letters, numbers, and symbols), while 73 students have not followed the best practices. Seven participants have not shown responded. These findings indicate that while many students adhere to secure password guidelines, a substantial number still use weak passwords, potentially exposing their accounts and devices to security risks.

- **Objective 3**: To determine the students are using the best practices in creating passwords such as in avoiding their personal information and avoiding the character diversity, and how often students change their passwords.

The results from Table.5 show of 100 students accepted that personal information like name, date of birth or other identical information are used in their password, where 61 students didn't, and six students did not respond. From this analysis, it shows that most student passwords can easily be hacked or predicted, which is a security risk.

Regarding students changing password habits regularly, only 40 students agreed to changing the password frequently, whereas the majority of 122 students agreed to not change the password regularly, and five students did not respond, increasing vulnerability to cyber threats.

Table.5. Personal information and Change Frequency

Password contains personal information		
Yes	**No**	**Missing**
100	61	6

Frequently change your passwords		
Yes	**No**	**Missing**
40	122	5

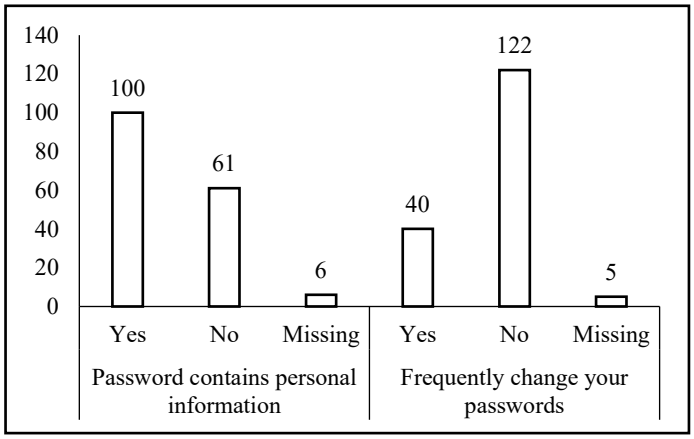

Fig.2. Password Personal information and Change Frequency Analysis

- **Objective 4**: To Determine whether students use the same password for multiple accounts

The result from Table.6 signifies that 72 students reuse the password in multiple platforms like online banking, Gmail, etc., where 91 students do not use the same password for different accounts and four student responses are missing. This is significant that the portion of students are engaging in risky password management practices, which could increase their vulnerability to cyber threats.

Similarly, 77 students agreed to share the password with family members and friends, where 86 students keep password as private, and four student responses are missing. Password sharing weakens security by increasing the chances of unauthorized access.

Table.5. Password Reuse and Disclosure Analysis

Same password for websites / online banking and other		
Yes	**No**	**Missing**
72	91	4
Disclosed passwords to friends or family		
Yes	**No**	**Missing**
77	86	4

The result from Table.5 signifies that 72 students reuse the password in multiple platforms like online banking, gmail, etc., where 91 students do not use the same password for different accounts and four student responses are missing. This is significant that the portion of students are engaging in risky password management practices, which could increase their vulnerability to cyber threats.

Similarly, 77 students agreed to share the password with family members and friends, where 86 students keep password as private, and four student responses are missing. Password sharing weakens security by increasing the chances of unauthorized access.

- **Objective 5**: To find out how students maintain their passwords.

The Fig.3 shows that 80 students declared to write down or save the password in a notebook, phone, computer, or somewhere else, while 83 students did not engage in this practice, and four student responses are missing. Storing passwords can be risky if not done securely, making it crucial to use encrypted storage methods.

Among those who saved their passwords, 77 students reported encrypting them, while 86 students did not encrypt their saved passwords. This indicates that a significant number of students store their passwords in a potentially vulnerable format.

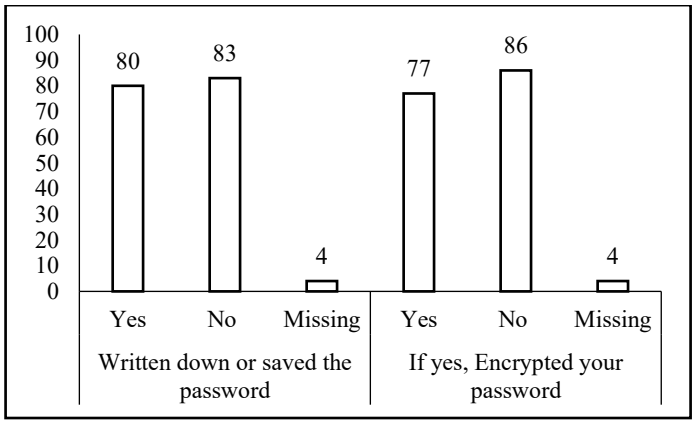

Fig.3. Password Storage and Encryption Analysis

6. DISCUSSION

The study findings show a significant gap among the students' awareness of password security and the real practices. Most of the students agreed on the importance of password security on their android devices, where a proportion of the students did not agree to use the password or using a weak password [1], [16]. Furthermore, quite a lot more students using the same password across various platforms, this increases the risk of unauthenticated access and proved in much recent research (Chan et al., 2017).

The study further observed a number of students use their personal information in passwords. This tradition links to increase vulnerability to cyber threads and attacks where it helps to easily predict the passwords are more susceptible to brute-force and dictionary attacks [4]. Students should have general awareness of the password security risks, but most of the students do not regularly change their passwords, this prolongs exposure to potential cyber threats [14].

Some students make use of storing the password in the encrypted format, but a large portion of the students store the password in a unsecure format. This attitude led to significant risks and shows the importance of password management skills among students [9]. Another worry is about password sharing where a significant number of students are in habit with family members or friends, this behavior determines personal password security and the probability of unauthorized access increase [13].

Interestingly, a large number of students believe that passwords are effective in protecting the information in digital devices, where some students remain suspicious of their effectiveness. This contradiction reflects from other researchers

state the facts of security measure does not always translate to ensure secure behaviors [3].

The research finding shows the importance of having the awareness of cyber security curriculum within educational institutions. Many researchers stated that by having the cyber security curriculum it will promote the students to know the importance of multi-factor authentication and will encourage the students to have the best practices in password security in digital platforms [12], [15].

7. CONCLUSION

This study highlights the important gap among the students' awareness of password security and the regular practices. Most of the students know the importance of having a strong password, but a significant number of students are in risk behaviors by reusing their passwords in different platforms, frequently not changing their password and sharing their password with family members or friends. Furthermore, most of the students are storing their passwords in an insecure manner. These results are important for the necessity of cyber security programs and awareness campaigns in educational institutions to raise the password security management practices. Through integration of password security programs and awareness campaigns with the curriculum, the students will have an opportunity to adopt multi-factor authentication and will encourage regular password updates [7].

8. RECOMMENDATIONS

1. Incorporate Cyber Security Awareness into the course [17].
2. Encourage the usage of Password Manager techniques [5].
3. Implementation of multi-factorial authentication on the college official platforms [6].
4. Develop a clear Cyber Hygiene policy for students [18].
5. Promote Password Periodic Security Check-Ups [11].

REFERENCES

[1] Ali Senol, Tarik Talan and Cemal Akturk, "A Research on University Students' Awareness of Cyber Security: Case Study of Password Usage", *Proceedings of International Conference on Innovative Studies of Contemporary Sciences*, pp. 46-56, 2021.

[2] Laszlo Bottyan, "Cybersecurity Awareness among University Students", *Journal of Applied Technical and Educational Sciences*, Vol. 13, No. 4, pp. 1-11, 2023.

[3] Altarawneh Mostafa, Thunibat Ahmad, Almajali Mohmmad Alzriqat, A. Naif and Alazzam Seif, "Cybersecurity Awareness among School Students: Exploring Influencing Factors, Legal Implications and Knowledge Gaps", *International Journal of Innovative Research and Scientific Studies*, Vol. 8, pp. 1516-1529, 2025.

[4] Bryant Kay and Campbell John, "User Behaviours Associated with Password Security and Management", *Australasian Journal of Information Systems*, Vol. 14, pp. 1-8, 2006.

[5] Chaudhary Sunil, Schafeitel-Tahtinen Tiina, Helenius Marko and Berki Eleni, "Usability, Security and Trust in Password Managers: A Quest for User-Centric Properties and Features", *Computer Science Review*, Vol. 33, pp. 69-90, 2019.

[6] Colnago Jessica, Devlin Summer, Oates Maggie, Swoopes Chelse, Bauer Lujo, Cranor Lorrie and Christin Nicolas, "It's not Actually that Horrible: Exploring Adoption of Two-Factor Authentication at a University", *Proceedings of International Conference on Human Factors in Computing Systems*, pp. 1-11, 2018.

[7] Constance Mouwers-Singh and Tichaona Buzy Musikavanhu, "A Narrative Review on Enhancing Cybersecurity in Higher Education Institutions: The Role of Continuous Training and Awareness", *Expert Journal of Business and Management*, Vol. 12, No. 2, pp. 67-73, 2024.

[8] M. Fagan, Y. Albayram, M.M.H. Khan and R. Buck, "An Investigation into Users' Considerations towards using Password Managers", *Human-Centric Computing and Information Sciences*, Vol. 7, No. 12, pp. 1-20, 2017.

[9] Fernando Prageeth, D. Dissanayake, S. Dushmantha, Liyanage Chamara and Karunatilake Chamila, "Challenges and Opportunities in Password Management: A Review of Current Solutions", *Sri Lanka Journal of Social Sciences and Humanities*, Vol. 3, pp. 9-20, 2023.

[10] D. Florencio and C. Herley, "Where Do Security Policies Come From?", *Proceedings of International Symposium on Usable Privacy and Security*, pp. 1-14, 2010.

[11] M.T. Gaata, Y.M. Mohialden and N. Mahmood Hussien, "Enhancing the Security of Information Systems using Iot Technology", *Journal La Multiapp*, Vol. 5, No. 4, pp. 322-335, 2024.

[12] Hussain Hamzha, "Password Security: Best Practices and Management Strategies", *SSRN*, pp. 1-5, 2022.

[13] Joris Ouytel, "The Prevalence and Motivations for Password Sharing Practices and Intrusive Behaviors among Early Adolescents' Best Friendships – A Mixed-Methods Study", *Telematics and Informatics*, Vol. 63, pp. 1-8, 2021.

[14] K.R. Kont, "Cybersecurity Behaviours of the Employees and Students at the Estonian Academy of Security Sciences", *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 4, No. 2, pp. 85-104, 2024.

[15] Maglaras Leandros, Ferrag Mohamed Amine, Janicke Helge, Buchanan William and Tassiulas Leandros, "Bridging the Gap between Cybersecurity and Reliability for Critical National Infrastructures", *Proceedings of International Conference on Cybersecurity*, pp. 1-11, 2023.

[16] Mihalovicsne Kollar Anita and Katona Jozsef, "Enhancing Password Security: Analyzing Password Management Practices among IT Students", *Proceedings of International Conference and Workshop on Electrical and Power Engineering*, pp. 1-8, 2024.

[17] Rahman Nuhan, I. Sairi, N. Zizi and Khalid Fariza, "The Importance of Cybersecurity Education in School", *International Journal of Information and Education Technology*, Vol. 10, pp. 378-382, 2020.

[18] U. Blase, J. Bees, S.M. Segreti, L. Bauer, N. Christin and L.F. Cranor, "Do Users' Perceptions of Password Security Match Reality?", *Proceedings of International Conference*

on Human Factors in Computing Systems, pp. 3748-3760, 2016.

[19] C. Wang, S.T. Jan, H. Hu and G. Wang, "Empirical Analysis of Password Reuse and Modification across Online Service", *Proceedings of International Conference on Cryptography and Security*, pp. 1-7, 2017.

[20] Xiaoguang Tian, "Unraveling the Dynamics of Password Manager Adoption: A Deeper Dive into Critical Factors", *Information and Computer Security*, Vol. 33, No. 1, pp. 117-139, 2025.