JIRBDAI

Journal of Institutional Research, Big Data Analytics and Innovation

PASSWORD HABITS AMONG UNDERGRADUATE STUDENTS: A CASE STUDY OF UNIDEL

Richard Omoefe Oveh[1*], Atomatofa, Emmanuel[2], and Mordi Nnamabia Godswill[3]

[1]Department of Information and Communication Technology, University of Delta, Agbor, Delta State, Nigeria
[2]Department of cybersecurity, Delta state university of science and technology, Ozoro, Delta state
[3]Department of Software Engineering, University of Delta, Agbor, Delta State, Nigeria
*Corresponding Author:richard.oveh@unidel.edu.ng

ABSTRACT There is a growing reliance on digital platforms in universities due to its transformative power in teaching, learning, engagement and collaboration opportunities. This increased use of digital platforms in universities has increased cybersecurity risks amongst university students due to weak or unsafe password habits. This study explores the password habits of university students, focusing on password strength, reuse, and management practices. A structured questionnaire was used to collect data. The target population were undergraduate students of University of Delta, Agbor. A total of 35 students participated. Participants were recruited through convenience sampling. 12 item questionnaire was developed to access various aspects of password behavior. The collected data were computed for each item using descriptive statistics showing frequencies and percentages. The findings reveal significant gaps in password security practices. Although many users are aware of the risks and express a preference for security, behavioral inconsistencies such as reliance on memorability over security, high rates of password sharing, and inconsistent practices in password uniqueness and updating suggest that there is a critical need for improved education, better password management tools, and alternative authentication methods that can reduce both the cognitive load and the risk of security breaches.` There is an urgent need for improved password management tools and alternative authentication methods that reduce the cognitive burden of password creation, streamline secure practices, and ultimately help users better protect their digital identities.

KEYWORDS: Password, Cybersecurity, University Students, Password Habits

I. INTRODUCTION

The growing reliance on digital platforms in higher education has transformed teaching and learning, offering innovative access, engagement, and collaboration opportunities [2]. These platforms, including e-learning systems and portals, have enhanced accessibility and convenience for students, staff, and faculty [1]. Digital technologies support blended learning and massive open online courses (MOOCs), revolutionizing educational delivery [3]. The adoption of digital platforms is driven by technological advances, increased internet connectivity, and demand for flexible, personalized learning experiences [2]. However, this shift also presents challenges for universities [2]. Digital platforms have facilitated internationalization in higher education, enabling virtual internationalization and Collaborative Online International Learning (COIL) programs [3]. As higher education institutions continue to embrace digital platforms, they are reshaping the educational landscape and expanding access to learning resources globally [1, 2]. Weak passwords pose significant risks to cybersecurity, including data breaches and identity theft. Studies have shown that even highly intelligent individuals may use weak passwords, suggesting that intelligence alone does not guarantee password strength [4]. Password reuse across multiple accounts increases vulnerability, as demonstrated by a University of Chicago incident where compromised Chegg accounts led to unauthorized access of university accounts [5]. Personal characteristics, such as personality

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15670059

traits and general risk-taking behavior, can predict an individual's likelihood of engaging in risky cybersecurity practices, including the use of weak passwords [7]. The proliferation of multiple accounts requiring passwords has exacerbated the challenge of creating and managing secure passwords, with users often prioritizing memorability over security [6]. These findings highlight the need for improved password management strategies and user education to mitigate the risks associated with weak passwords.

Research indicates that students, particularly vulnerable youth, are at increased risk of excessive internet use and cybersecurity threats due to high digital engagement and perceived invulnerability. Psychological vulnerability combined with higher levels of digital engagement can lead to negative outcomes [8]. College students are especially susceptible to internet addiction due to developmental factors, easy access, and expected use [9]. While big data can help track and support vulnerable students' engagement, it also raises privacy concerns [10]. Perceived vulnerability to cybersecurity risks is influenced by information security attitudes and behaviors, with self-perceived competence potentially leading to overconfidence [11]. These findings highlight the complex interplay between psychological factors, digital literacy, and online behaviors among students, emphasizing the need for interventions that consider both psychological and digital literacy aspects to address excessive internet use and cybersecurity risks. This paper evaluates password practices among UNIDEL undergraduates to identify factors influencing poor password habits (e.g., convenience, lack of awareness). This would inform cybersecurity education policies tailored to African university contexts.

II. RELATED WORKS

Studies consistently show poor password habits among users worldwide. A large-scale study of 500,000 users found that a typical user manages only about seven distinct passwords, reusing them across multiple sites [12].Users often choose weak, easily guessable passwords like words, names, or birthdates for memorability [13]. A survey revealed that about one-third of users chose weak passwords, including personal information or dictionary words [14]. Despite the importance of strong passwords, little progress has been made in password management practices over the past 35 years [13]. Research has shown a discrepancy between users' intentions and actual practices when creating passwords, with misconceptions and convenience fostering bad habits [15]. While password policies and checkers can help users create stronger passwords, further research is needed to determine their effectiveness and user-friendliness [13]. Recent studies provide insights into password behaviors among Nigerian students and staff. A survey in southeastern Nigeria found that account compromise was relatively uncommon, with respondents reporting generally positive experiences with password usage [16]. This contrasts with global norms of weak passwords, as 93% of participants in another Nigerian study created weak passwords [17]. However, password protection was reported as the most common security practice among Nigerian university staff [16], suggesting institutional recognition of its importance. Cultural factors may influence password behaviors, with some ethnic groups creating stronger passwords than others [17]. Comparatively, a South African study found that over 60% of students actively used passwords to protect their data [18]. Research has also shown correlations between demographic factors and password strength, with computer science students creating stronger passwords than business students [19] .

A. THEORETICAL FRAMEWORK

Protection Motivation Theory (PMT) has been applied to understand and improve online security behaviors, particularly password practices. Studies have shown that PMT-based interventions can increase users' intentions to change breached passwords and lead to actual password changes, though the effects may be small [20]. Factors such as threat appeals, coping appeals, security attitudes, and time since breach influence password change behaviors [20]. PMT-based fear appeals and password training can improve compliance with password guidelines and result in stronger passwords, but long-term effects on compliance intentions may be limited [21]. Coping appraisal variables, including habit strength, res4can enhance its explanatory power for understanding online security behaviors [22].

B. CONTEXTUAL GAPS

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15670059

Research on password practices in Nigerian universities is limited, but some studies provide insights. A survey of university staff and students in southeastern Nigeria found that account compromise was not common, and password experience was generally positive, unrelated to age or education level [16]. A broader survey of cybersecurity practices in Nigeria indicated moderate knowledge but poor practices such as weak passwords and password sharing [23]. While not specific to Nigeria, a study of university passwords in the US found correlations between demographic factors and password strength, with computer science users creating stronger passwords than business school users [24]. These findings highlight the need for further research and improved cybersecurity awareness in Nigerian universities and beyond.

III. METHODOLOGY

This study employed a quantitative research design to systematically investigate the password habits of university students. The approach was chosen to provide measurable, numerical data that could be analyzed to identify trends, patterns, and correlations in password-related behaviors. Quantitative methods are particularly well-suited for studies aiming to generalize findings across a specific population. A structured questionnaire was used to collect data. The target population were undergraduate students of University of Delta, Agbor. A total of 35 students participated. Participants were recruited through convenience sampling, announcements in undergraduate classes and distribution in whatsApp groups. The survey was administered online using Google Forms which was chosen for its ease of use and broad accessibility. All responses were collected anonymously with no identifying information. 12 item questionnaire was developed to access various aspects of password behavior. The list of the questions are shown below:

1. What motivates your choice of password? (Rank the following in order of importance)
2. Do you feel stressed or overwhelmed when asked to create a new password?
3. How much effort do you put into creating a "strong" password?
4. How often do you think about the risks of weak password habits?
5. If you had to choose between security and convenience, which would you prioritize?
6. Do you think it’s necessary to have unique passwords for each account?
7. How confident are you in the strength of your passwords?
8. Do you use multi-factor authentication (MFA) for your accounts?
9. Have you ever been a victim of a cyberattack or account compromise?
10. Have you ever shared your passwords with others?
11. How do you store or remember your passwords?
12. How often do you change your passwords?

The questionnaire was reviewed by an information security faculty for content validity and was pilot tested with a small group of students (n-5). Minor adjustments were made based on pretest feedback. The collected data were computed for each item using descriptive statistics. Frequencies and percentages for the categorical responses are shown below.

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15670059

IV. RESULTS AND DISCUSSION

The results indicate notable gaps in password security practices among the sample population, expanding on each finding:

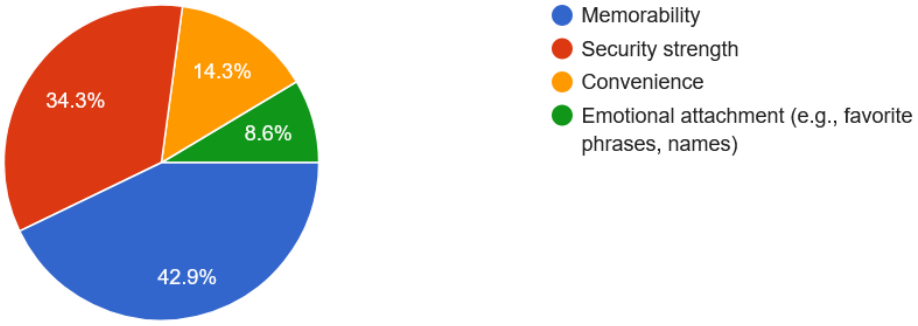

Figure 1: What Motivates your Choice of Password?

From Figure 1, 34.3% opined that security strength motivated their choice of password, 42.9% said memorability, 14.3% convenience and 8.6% emotional attachment. This highlights students' priorities and motivations when choosing passwords, revealing a tension between security, usability, and personal preferences.

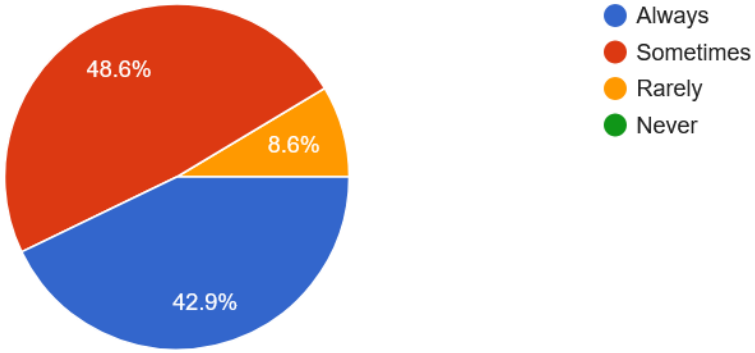

Figure 2: Do you feel stressed or overwhelmed when asked to create a new password

From Figure 2, 48.6% of the respondents sometimes feel stressed or overwhelmed when asked to create a new password, 42.9% always and 8.6% rarely. This indicates that the process of creating new passwords is a significant source of frustration for users, which can contribute to overall password fatigue and may point to the need for simpler or alternative authentication methods.

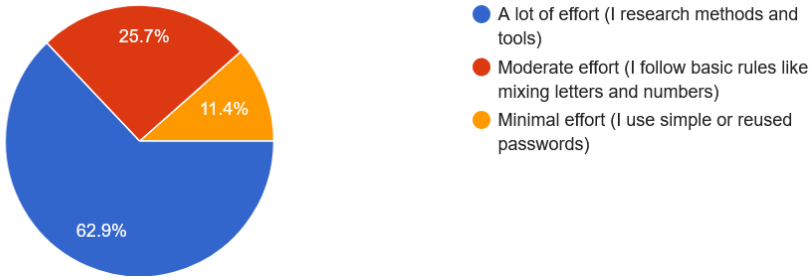

Figure 3: How much Effort do you put into Creating a Strong Password?

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15670059

From Figure 3, 62.9% of the respondents put a lot of effort in creating a strong password, 25.7% put in moderate effort and 11.4% put in minimal effort. This suggests a generally high awareness of the importance of robust passwords, though there remains a segment that may be at greater risk due to less effort.

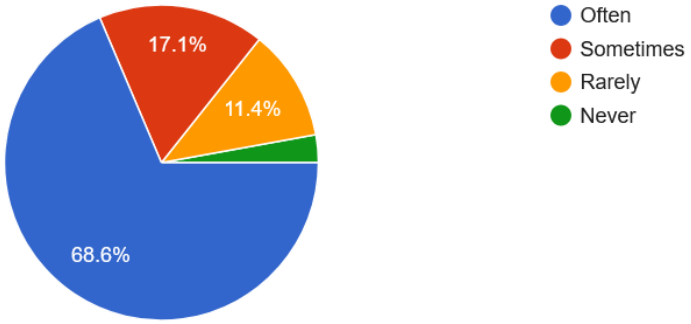

Figure 4: How Often do you Think about the Risks of Weak Password Habits

From Figure 4, 68.6% think about the risks of weak password often, 17.1% sometimes and 11.4% rarely think about these risks, indicating that while most users are proactive about security, there is still a minority that may be less vigilant.

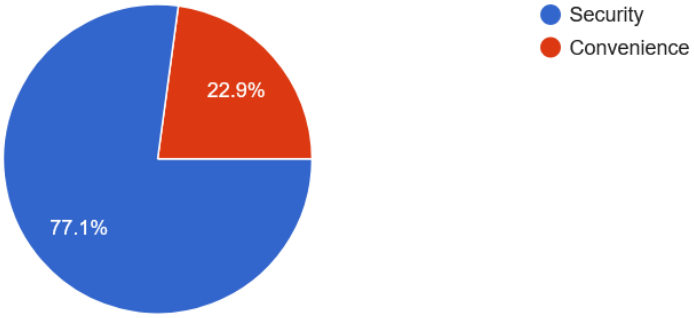

Figure 5: If you had to choose between Security and Convenience which, would you Prioritize

From Figure 5, 77.1% of the respondents would prefer security over convenience while 22.9% think otherwise. This indicates that most users value protecting their data and accounts, even if it means a slightly less seamless experience.

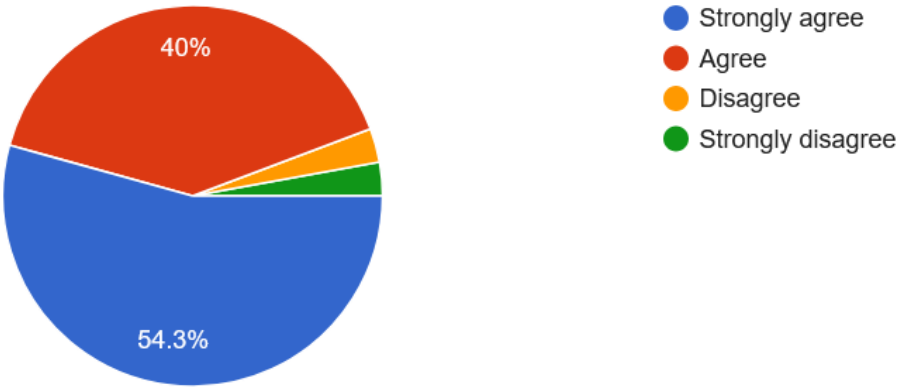

Figure 6: Do you think it's necessary to have unique passwords for each account?

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15670059

From Figure 6, 54.3% think it's necessary to have unique passwords for each account while 40.7% think otherwise. Suggesting that many users might still be reusing passwords and potentially exposing themselves to greater security risks.

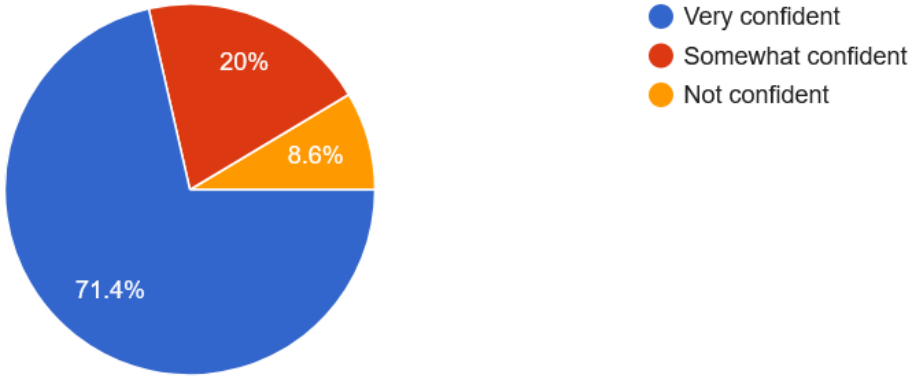

Figure 7: How Confident are you in the Strength of your Passwords?

From Figure 7, 71.4% of the respondents are very confident in the strength of their passwords, 20% are somewhat confident, while 8.6% are not confident. This suggests that overall, users generally trust the robustness of their passwords, though there's still a minor group who may feel vulnerable.

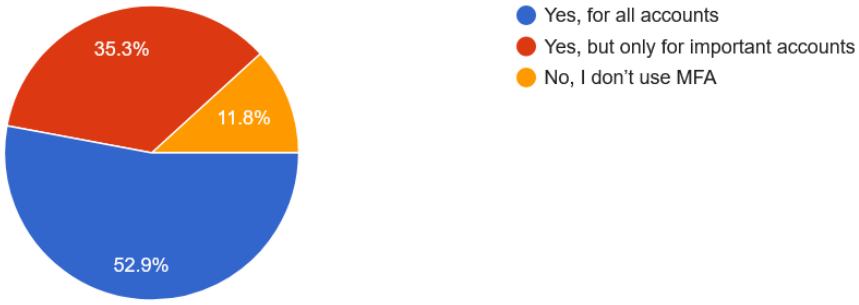

Figure 8: Do you use Multi-Factor Authentication for your Accounts?

From Figure 8, 52.9% use multi-factor authentication for their accounts, 35.3% use it for important accounts only, while 11.8% don't. This indicates a generally positive trend toward adopting additional security measures, though there remains a segment that could benefit from broader MFA implementation.

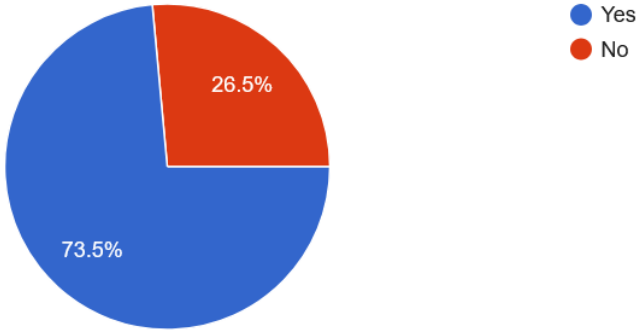

Figure 9: Have you ever been a victim of a Cyberattack or Account Compromise?

From Figure 9, 73.5% of the respondents have been a victim of a cyberattack or account compromise before, while 26.5% haven't. It shows that a significant majority of respondents (73.5%) have experienced a cyberattack or account compromise, which underscores just how widespread cyber threats are. This high

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15670059

incidence highlights the urgent need for improved cybersecurity measures, as nearly three-quarters of users have been directly impacted by these breaches.

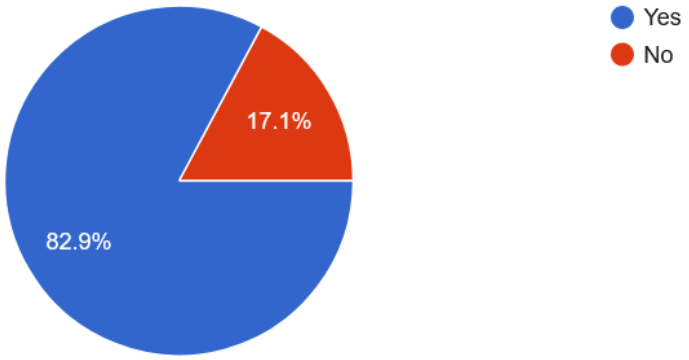

Figure 10: Have you ever shared your password with others

From Figure 10, 82.9% of the respondents have shared their password with others before while 17.1% haven't. It shows that a vast majority of respondents (82.9%) have shared their passwords with others at some point, indicating that password sharing is a very common behavior among users. This high rate of sharing can significantly increase security risks, as shared passwords may be more easily compromised, compared to the 17.1% who have not shared their passwords.

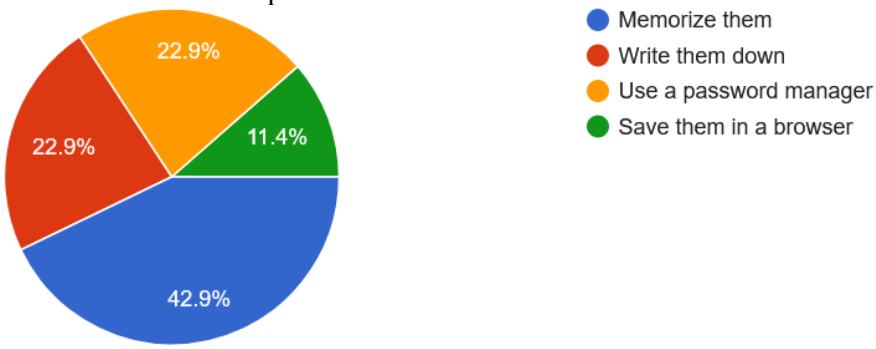

Figure 11: How do you store or remember your passwords?

From Figure 11, 42.9% of the respondents memorize their passwords, 22.9% write them down, 22.9% use a password manager while 11.4% save them in a browser. This variety indicates that while many trust their memory, a significant number still use physical or digital aids (each with its own security implications).

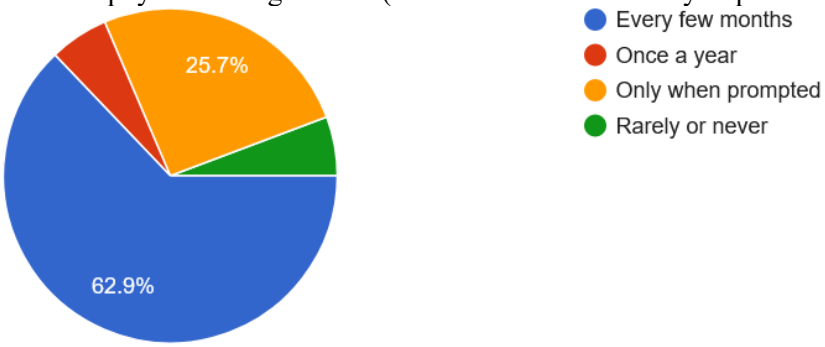

Figure 12: How often do you change your passwords?

From Figure 12, 62.9% change their passwords every few months, 25.7% only when prompted and 11.4% seldom change their passwords. Indicating that while many users are proactive about refreshing their

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15670059

credentials, a significant minority may be more vulnerable to prolonged exposure if their passwords become compromised.

The results paint a picture of a user base that is caught in a balancing act between security, convenience, and usability. On one hand, when it comes to choosing a password (Figure 1), a large portion of respondents (42.9%) opt for memorability, with only 34.3% driven by security strength. This suggests that while users do value security, the ease of recall often takes precedence, potentially leaving room for weak or reused passwords. This trade-off is further compounded by the emotional burden observed in the process of password creation (Figure 2): nearly 91.5% of respondents (48.6% sometimes and 42.9% always) experience stress or overwhelm when creating a new password. Yet, despite this stress, most users invest significant effort into crafting strong passwords (Figure 3, with 62.9% putting in a lot of effort), which indicates an awareness of the importance of password robustness.

In Figure 4, a healthy 68.6% regularly consider the risks of weak passwords, suggesting that many are aware of the potential dangers. This concern is reflected in Figure 5, where an overwhelming 77.1% prioritize security over convenience. Indicating that, in theory, users would rather endure inconvenience than risk a breach. However, there are notable inconsistencies in practices. For instance, while 54.3% believe in having unique passwords for each account (Figure 6), a sizable 40.7% do not, which could explain the high incidence of cyberattacks (73.5% of respondents reported having been victims of cyberattacks or account compromises in Figure 9). Furthermore, the high rate of password sharing (82.9% in Figure 10) further exposes users to vulnerabilities, even if they feel confident about their own password strength (Figure 7 shows 71.4% are very confident).

When it comes to password management, the methods vary considerably (Figure 11): 42.9% rely on memory, while 22.9% each write them down or use a password manager, and 11.4% rely on browser storage. These choices carry different risks as memorization can lead to forgotten passwords or reuse, while written or browser-stored passwords can be physically or digitally compromised. Finally, while 62.9% of users change their passwords every few months (Figure 12), a combined 37.1% either change them only when prompted or rarely, potentially leaving a window of exposure if a password is compromised. Together, these findings reveal significant gaps in password security practices. Although many users are aware of the risks and express a preference for security, behavioral inconsistencies—such as reliance on memorability over security, high rates of password sharing, and inconsistent practices in password uniqueness and updating—suggest that there is a critical need for improved education, better password management tools, and alternative authentication methods that can reduce both the cognitive load and the risk of security breaches.

V. CONCLUSION

The results reveal a complex landscape of password security practices among the respondents. On one hand, there is clear awareness and concern about cybersecurity and overwhelmingly prioritize security over convenience. A majority invest significant effort in crafting strong passwords and express high confidence in their own password strength. However, these positive attitudes are undermined by inconsistent behaviors. Many users still favor memorability over pure security and report feeling stressed or overwhelmed when creating new passwords, which can lead to shortcuts like reusing passwords and sharing them with others. The fact that a large proportion of respondents have experienced cyberattacks or account compromises underscores the real-world impact of these risky practices. Moreover, while most users update their passwords periodically, a significant minority do so only when prompted or rarely, further increasing their exposure to threats. These findings highlight a critical gap between users' intentions to secure their accounts and their actual practices. There is an urgent need for improved password management tools and alternative authentication methods that reduce the cognitive burden, streamline secure practices, and ultimately help users better protect their digital identities.

REFERENCES

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.15670059

1. Jones, K.D. (2004) 2005: The Year of the Digital Campus. *T.H.E. Journal Technological Horizons in Education, 32*, 32.
2. Zhao, H. (2024) Digital Platforms in Higher Education: Opportunities, Challenges, and Strategies. Proceedings of the 8th International Conference on Economic Management and Green Development. 118-122. DOI: 10.54254/2754-1169/116/20242447
3. Lima, C. D., Bastos, R. C., and Varvakis, G. (2020) Digital Learning Platforms: An Integrative Review to Support Internationalization of Higher Education. Edur Educação em Revista. 2020; 36:e232826, DOI: http://dx.doi.org/10.1590/0102-4698232826
4. Roig, J.V. (2018). Do Smarter People Have Better Passwords? *ArXiv, abs/1805.02931*.
5. Nisenoff, A., & Golla, M. (2023). Measuring the Risk Password Reuse Poses for a University.
6. Weber, J.E., Guster, D.C., Safonov, P., & Schmidt, M.B. (2008). Weak Password Security: An Empirical Study. *Information Security Journal: A Global Perspective, 17*, 45 - 54.
7. Kennison, S. M., and Chan-Tin (2020) Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. Frontiers in Psychology. 11
8. Helsper, E.J., & Šmahel, D. (2020). Excessive internet use by young Europeans: psychological vulnerability and digital literacy? *Information, Communication & Society, 23*, 1255 - 1273.
9. Kandell, J.J. (1998). Internet Addiction on Campus: The Vulnerability of College Students. *Cyberpsychology Behav. Soc. Netw., 1*, 11-17.
10. Watson, R.J., & Christensen, J.L. (2017). Big data and student engagement among vulnerable youth: A review. *Current Opinion in Behavioral Sciences, 18*, 23-27.
11. Debb, S.M., & McClellan, M.K. (2021). Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. *Cyberpsychology, behavior and social networking, 24 9*, 605-611.
12. Florêncio, D. and Herley, C. (2007) A Large-Scale Study of Web Password Habits. Proceedings of the 16th International Conference on World Wide Web, Banff, May 2007, 657-666. http://dx.doi.org/10.1145/1242572.1242661
13. Taneski, V., Heričko, M., & Brumen, B. (2014). Password security — No change in 35 years? *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1360-1365.
14. Furnell, S. & Bär, N. (2013) Essential Lessons Still Not Learned? Examining the Password Practices of End-Users and Service Providers . Springer-Verlag Berlin Heidelberg, 217–225.
15. Hanamsagar, A., Woo, S.S., Kanich, C., & Mirkovic, J. (2018). Leveraging Semantic Transformation to Investigate Password Habits and Their Causes. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*.
16. Ezugwu, A.O., Ukwandu, E.A., Ugwu, C., Ezema, M., Olebara, C.C., Ndunagu, J.N., Ofusori, L.O., & Ome, U. (2023). Password-Based Authentication and The Experiences of End Users. *ArXiv, abs/2305.18909*.
17. Kawu, A.A., Orji, R., Awal, A., & Gana, U.M. (2018). Personality, culture and password behavior: a relationship study. *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*.
18. Lubbe, S., & Klopper, R. (2009). The Problem with Passwords. http://thecipherbrief.com/article/problem-passwords,
19. Mazurek, L. M., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Kelley, P.G., Shay, R., and Ur, B. (2013) Measuring Password Guessability for an Entire University. ACM, 173-186, http://dx.doi.org/10.1145/2508859.2516726.
20. Zou, Y., Le, K., Mayer, P., Acquisti, A., Aviv, A.J., and Schaub, F. (2024) Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory. ACM Trans. Computer Human Interaction. 31 (5) 63.1 - 63.45. https://doi.org/10.1145/3689432
21. Mwagwabi, F. (2015). A protection motivation theory approach to improving compliance with password guidelines. Doctor of Philosophy (PhD), Murdoch University
22. Tsai, H. S., Jiang, M., Alhabash, S., LaRose,R., Rifon, N. J., and Cotten, S. R. (2016) Understanding online safety behaviors: A protection motivation theory perspective, Computers & Security, 59, 138-150. https://doi.org/10.1016/j.cose.2016.02.009.
23. Rufai, A., Modi, S., & Wadata, B. (2020). A Survey of Cyber-Security Practices in Nigeria. International Research Journal of Advanced Engineering and Science. 5(3) 222-226
24. Mazurek, L. M., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, F.L., Kelley, P.G., Shay, R. and Ur B. (2013) Measuring Password Guessability for an Entire University. ACM, 173-186

https://doi.org/10.5281/zenodo.15670059