IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

STRENGTHENING PASSWORD MANAGEMENT

Akansha Bhagat, Somashekhara Reddy D

Master's Student-Forensic Science, Assistant Professor Department of CSE-GEN

Department of Forensic Science

Jain (Deemed-to-be University) Bangalore, India

Abstract: This research investigates password management behaviors and issues for students in forensic science. Although cybersecurity awareness is on the rise, most users continue risky practices such as password reuse, poor password generation, and underutilization of security features like password managers or two-factor authentication. A systematic survey among 200 participants was carried out to determine password practices, security knowledge, and typical challenges encountered by users. Findings indicated high memory reliance, low password manager adoption, and a disparity between awareness and action for secure behaviors. The results indicate the necessity of more robust cybersecurity education and the creation of easy-to-use password management tools to alleviate human error and enhance digital Hygiene.

IndexTerms **– Cybersecurity Awareness, Digital Hygiene, Password Management, Password Reuse, Two-Factor Authentication**

I. INTRODUCTION

In the digital era, passwords are still the most prevalent means of verification. Still, lax password habits continue to undermine individual and organizational security. Prevalent problems involving reuse of passwords, weak password generation, and inattention to the use of protective mechanisms such as two-factor authentication account for a large proportion of data breaches and unauthorised access.

A number of studies have illustrated these issues. Golla and Durumuth (2018) documented that while password managers provide heightened security, there are many individuals who are afraid to use them because of issues related to usability and trust. Chiasson et al. (2019) investigated the issue of password fatigue and advised biometrics and 2FA as substitutes. Farke et al. (2020) stressed that the reuse of passwords is still the biggest weakness of digital ecosystems.

The present study is interested in assessing password management behavior, awareness, and challenges among learners. Through survey feedback from 200 respondents, the research hopes to determine patterns of behavior, draw attention to misconceptions, and suggest strategies to enhance password hygiene. The findings are hoped to inform user-oriented cybersecurity measures and awareness programs.

II. MATERIALS AND METHODS

It applied descriptive, survey research to measure the password management behavior, levels of awareness, and difficulties amongst the students. It used a well-structured questionnaire with multiple-choice, Likert-scale, and open questions formatted through Google Forms.

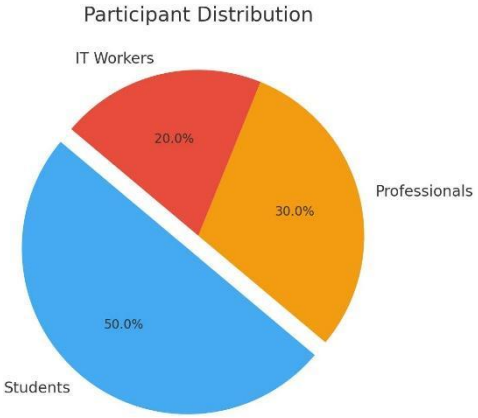
The survey addressed important topics like password generation habits, how often passwords are changed, utilization of passwords managers, dependence upon memory or external devices, and knowledge and utilization of two-factor authentication. Questions were worded to capture both behavior and self-reported issues.

200 participants were recruited through convenience sampling, with the main focus being students from forensic science and similar academic backgrounds. The link to the survey was distributed via academic networks, email, and WhatsApp groups to collect a diverse response pool.

Voluntary and anonymous participation was ensured. No personal identifiable information was gathered. Informed consent was ensured prior to submission, and the study complied with ethical principles for handling user data and confidentiality.

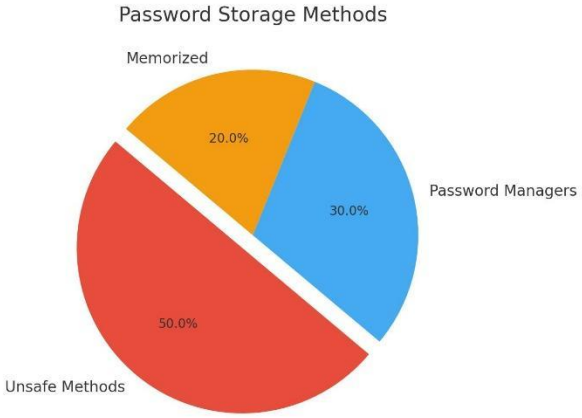
III. RESULTS

The data collected from 200 participants gave an overview of password management practices, awareness, and user challenges. When questioned about how often they changed their passwords, 40% of the respondents reported updating their passwords once in six months, 30% did so once a year, while 30% admitted to rarely or never changing their passwords. These findings highlight a general lack of regular password maintenance among users, which can increase vulnerability to cyber threats.



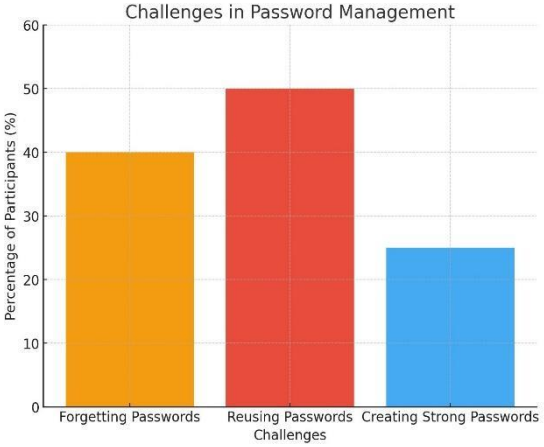
(Figure 1)

About 30% of the participants believe they create strong passwords, whereas 70% admitted using easy-to-guess passwords for convenience. Majority 50 of participants uses unsafe methods, 20% note it down somewhere or memorizes, where 30% use password manager applications. Majority of respondents reported using the same password for multiple accounts, which indicates a higher risk of security breaches. *(Figure 2)*



(Figure 2)

Participants where further asked about the challenges they experience in managing passwords. The most commonly reported issue was forgetting passwords (40%), followed by difficulty in creating strong passwords. Additionally, 50% of users found frequent password updates inconvenient, and expressed reluctance or lack of knowledge in using password managers. These responses suggest that password fatigue, cognitive load, and lack of awareness continue to hinder the adoption of secure practices. *(Figure 3)*



IV. DISCUSSION

The findings of this study indicate that a significant portion of users still engage in secure password practices, despite increasing awareness of cybersecurity threats. The most concerning trend is that a majority of participants rarely update their passwords, with only a small percentage following a regular update routine. This behavior increases susceptibility to brute-force attacks, credential stuffing, and other forms of unauthorized access. The preference for convenience over security, as seen in the reuse of the same password across multiple platforms, highlights a common yet dangerous habit among users.

These results align with previous studies. Farke et al. (2020) similarly found that password reuse remains a persistent vulnerability. Additionally, Golla and Durmuth (2018) emphasized that while password managers offer enhanced security, users often avoid them due to usability concerns or mistrust in storing sensitive information digitally. This was reflected in the present study, where only a minority of participants used password managers, while most relied-on memory or physical notes.

Another important observation from the study is the cognitive burden users face-including forgetting passwords, difficulty creating strong credentials, and the pressure of frequent password resets. Chiassson et al. (2019) described this phenomenon as "password fatigue", which affects user compliance with best practices. The feedback from participants in this survey reinforces the need for simplified tools and better user education in password management.

The discussion of 2FA also presents an opportunity for improvement. Although awareness levels are gradually increasing, the implementation remains limited. This suggests a behavioral gap between what users know and what they apply, reinforcing the importance of not only educating users but also designing more user-friendly cybersecurity solutions.

The study emphasizes that technical solutions alone are not enough. Human behavior, usability, and user perception play a crucial role in security effectiveness. Bridging this gap through targeted awareness programs and simplified password management programs and simplified password management solutions is essential for improving cyber hygiene at the individual level.

V. CONCLUSION

This research demonstrates a clear disconnect between users' awareness about cybersecurity and their actual password behaviors. Even though they know better, most of the study participants reuse passwords and do not change them often. This highlights the importance of improved user education and implementation of secure yet easy-to-use tools such as password managers and 2FA. Digital hygiene can be made more secure not just through technical measures but also through a shift in user behavior.

VI. ACKNOWLEDGEMENT

The author extends sincere gratitude to the guide **Prof. Somashekhara Reddy D,** for the continuous support, valuable guidance, and encouragement throughout the course of this research work. The author also expresses heartfelt thanks to the faculty members of the Department of Forensic Science, Jain University, for their constructive feedback and motivation.

Special appreciation goes to the participants and respondents who contributed their time and insights, making this research possible. Lastly, the author is thankful to the institution for providing the resources and environment necessary to carry out this study successfully.

VII. REFERENCES

[1] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. *IEEE Symposium on Security and Privacy, 553-567.*

[2] Chiasson, S., Van Oorschot, P. C., & Biddle, R. (2019). A usability study and critique of two password managers. *ACM Transactions on Information and System (TISSESC), 12(4), 1-38.*

[3] Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. *NDSS Symposium 2014, 1-15.*

[4] Farke, F.M., Krombholz, K., & Riegar, M. (2020). The reality of attacks on password-protected devices. *Proceedings on Privacy Enhancing Technologies, 2020(4), 460-479.*

[5] Florencio, D., & Herley, C. (2010). Where do security policies come from? *Proceedings of the Sixth Symposium on Usable Privacy and security (SOUPS), 1-14.*

[6] Golla, M., & Durmuth, M. (2018). On the security, usability, and adoption of two-factor authentication mechanisms. *ACM Conference on Human Factors in Computing Systems (CHI) 1-14.*

[7] Krombholz, K., Busse, K., Pfeffer, K., & Smith, M. (2021). "I have no idea what I'm doing"-On the usability of deploying security protocols. *IEEE Symposium on Security and Privacy, 284-301.*

[8] Souza, D.L.D., de Oliverira, T.R., Ferreira, A., & de Souza, J.N. (2022). Passwordless authentication. A survey and security analysis. *Journal of Information Security and Applications, 64, 103039.*

[9] Stobert, E., & Biddle, R. (2014). The password life cycle: User behavior in managing passwords. *Proceedings of the Tenth Symposium on Usable Privacy and Security (SOUPS), 243-255.*

[10] Wash, R. (2010). Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security 9soups0, 1-16.*