The Password Behaviour Paradox: Understanding the Gap Between Cybersecurity Knowledge and Secure Password Practices

Vaishnavi Ajit Sawant[1], Vedant Umesh Kadam[2], Swamini Kadam[3], Omkar Sherkhane[4]
[1,2,3,4]*Pillais College of Arts Commerce and Science Autonomous*

I. INTRODUCTION

Text-based passwords stay one of the common ways people log in. I have noticed that many people still struggle with password habits. Passwords also act as the shield for digital privacy, money records and school or company data across the internet. Because digital services grow in schools, businesses and personal life people must handle password-protected accounts and type their passwords often. That means security now depends a lot on people how well they can create, manage and follow safe password habits. With constant security lessons and tips on password care a clear gap stays between what people know and what they actually do. This gap is called the Password Behaviour Paradox.

Studies show that knowing about security does not always lead people to use password habits. People still show risky password habits even while they know the simple security rules. Examples are reusing the password on many sites, which lets attackers use one breach to hit many accounts. People also pick patterns people can guess, like starting with a capital letter ending with numbers or using facts. They rarely change passwords and store passwords in places, such as plain-text notes, unencrypted files, paper notebooks or by giving passwords to others. Also, research finds an overconfidence bias: users think their password skills are good enough even while they do things that make passwords easy for automated attacks. All of this shows that making password security better needs more, than teaching. It must also tackle the habits that shape how people truly handle their passwords.

II. LITERATURE REVIEW

1. Foundations of Password Security Behaviour

1.1 Protection Motivation Theory

Protection Motivation Theory (PMT) offers a clear framework for understanding how people act in cyberspace. PMT shows that protective actions come from two steps: threat appraisal and coping appraisal. Threat appraisal looks at how serious a danger seems and how likely a user thinks they will be affected. Coping appraisal considers how effective a response is, how confident a user feels about doing it and how costly or difficult the response seems.

Studies on password security show that just seeing a danger does not always make users act safely. Zhang and McDowell discovered that how serious and how exposed users felt did not strongly predict whether users would choose passwords. Other research that uses PMT says that things like how effective users think a rule is and how hard it is to follow password rules can change users' security plans. This means that users may know the dangers of passwords but still skip safe habits when users think those habits are hard or uncomfortable.

1.2 Convenience and Rational Security

Password behaviour can also be explained by bounded rationality and the idea of Rational Security. Users often choose security actions while looking at limits like time, effort and how hard it is to remember many passwords. Research on password use found that users may see passwords as an extra cost that comes with doing their main tasks. Likewise, research on how users manage passwords shows that perceived benefits, convenience can drive risky actions like reusing passwords. Secure password behaviour may

rely not only on what users know but also on how convenient users think the suggested actions are.

2. Empirical Evidence on Password Behaviour

Password reuse is one of the studied risky practices. Studies show that users may reuse passwords or use ones on many accounts because this saves users effort when remembering many passwords. Studies also found patterns when creating passwords. For example, university students often put numbers and capital letters in the places even though their passwords meet the technical rules. This shows that following password rules does not always make passwords truly safe. Research with university students also shows that knowing about cybersecurity does not always lead to password habits. Website design and uneven password rules can further shape how users make and handle passwords.

3. The Knowledge–Behaviour Gap

A finding in the literature is that knowing about cybersecurity does not always turn into safe behaviour. Users may know that reusing passwords is risky yet keep reusing them because of convenience a feeling of personal danger or the effort needed to handle many passwords. Perceived risk is an important factor. A user may understand that weak passwords are harmful yet still think their own accounts will not be hit. At the time convenience can give a quick win that beats the imagined future danger. This creates the Password Behaviour Paradox: Users may know what safe password habits are but still do not do them.

4. Research Gap

Earlier studies looked at password awareness, perceived risk, convenience, password reuse and safe habits separately. The study still needs to see how these factors mix to explain the gap between what students know and what they do. Therefore, this study focuses on the link, between: Cybersecurity Knowledge → Perceived Risk and Convenience → Password Security Behaviour. The study aims to find out if knowing about cybersecurity is linked to password habits and if perceived risk and convenience explain why those who know still take risky password actions.

III. RESEARCH METHODOLOGY

Research Design

I intend to use a cross-sectional research design to investigate the relationship between cybersecurity knowledge and password behaviour among university students. The study focuses on addressing the Password Behaviour Paradox, which refers to the discrepancy between individuals' awareness of what constitutes secure passwords and their actual behaviour when managing multiple accounts. The conceptual framework employed in this study is based on Protection Motivation Theory (PMT) and Rational Security paradigm which highlights the influence of perceived cyber risk and convenience on users' decisions to adhere to or deviate from recommended password practices.

The study examines the potential association between cybersecurity knowledge, perceived cyber risk and convenience with password security behaviour. It proposes a conceptual model that seeks to establish if individual's cybersecurity knowledge influences their adherence to secure password practices as well as determine if perceived cyber risk and convenience moderate this relationship.

Sampling

The target population for this study consists of students pursuing higher-education and using multiple accounts and digital services. The sampling criteria include students who are at least 18 years old and currently enrolled in a college or university. I will employ a convenience sampling approach and distribute the questionnaires through student groups, social media and other digital platforms to recruit the target sample of 150 to 200 respondents.

The study will be based on voluntary participation with informed consent from all respondents.

Data Collection

The primary data described in this study will be collected using a 10-question online survey. The survey instrument will be designed to measure cybersecurity knowledge, perceived cyber risk, convenience and assess participant's password-related practices. The survey questions will focus on eliciting rich information regarding participants' attitudes and behaviours related to password use including reuse, changing frequency, perceived likelihood of account

compromise, use of additional security measures, and the impact of convenience on password choices. All questions will be formatted to allow respondents to provide answers using a five-point Likert scale.

The survey will not collect any sensitive information including passwords, usernames and other personally identifiable information. All information collected will be used strictly for research purposes and analysed in an anonymized form.

Data Analysis

Initial descriptive statistics including frequencies and percentages will be generated using Microsoft Excel. The findings will provide insights into the prevalent password behaviours among the studied population. I will use the Chi-Square test of independence to explore the relationship between each set of variables including cybersecurity knowledge and password reuse. This analysis will shed light on the association between the independent variables and the dependent variable and inform the next steps of data analysis.

Since many variables in the questionnaire will be measured using a Likert scale, I will apply Spearman's rank correlation to examine the relationships between cybersecurity knowledge, perceived cyber risk and convenience, and password security behaviour.

I will conduct a gap analysis to identify respondents that display a knowledge-behaviour gap in terms of their cybersecurity knowledge and corresponding practices. This analysis will support the identification of respondents who recognise secure password practices but fail to adopt them or choose to use insecure or convenience-based passwords.

Interpretation of results will rely on the statistical analysis and calculation of correlation coefficients and significance levels to determine the relationships between independent and dependent variables as well as provide support for the proposed conceptual model.

Ethical Considerations

The study will follow ethical guidelines and ensure voluntary participation, informed consent and confidentiality of collected information. Participants will be able to withdraw from the study at any time and will not be obliged to provide any sensitive or private information or actual passwords.

IV. DATA ANALYSIS

A sample of 150 responses was used to illustrate the analysis of the questionnaire. The responses were evaluated using frequency distributions, percentage analysis, cross-tabulation, Chi-Square testing, and Spearman's rank correlation.

The analysis revealed that 10.7% of respondents reported reusing passwords often or always, while 82.7% correctly identified a long and unique password as the safest option. Thus, it may be concluded that the recognition of passwords' secure practices may exist simultaneously with insecure password practices.

The perceived-risk responses revealed that 39.3% of respondents believed that an account compromise is likely or very likely, while 30.0% were unsure. Thus, it may be concluded that the personal perceived-risk of most respondents was not that high, which may have affected their attitude toward password practices.

Moreover, it may be seen that convenience plays an important role in password management. Indeed, when asked about how they managed multiple passwords, the biggest group selected using a password manager (41.3%), while others opted for using a few passwords, reusing the same passwords, and writing passwords down.

Finally, Spearman's rank correlation between the perceived risk and reuse of passwords revealed that a negative relationship existed between the two variables ($\rho = -0.241$, $p = 0.003$) in the simulated dataset. Thus, it may be said that the higher was the perceived risk, the lower was the reuse of passwords.

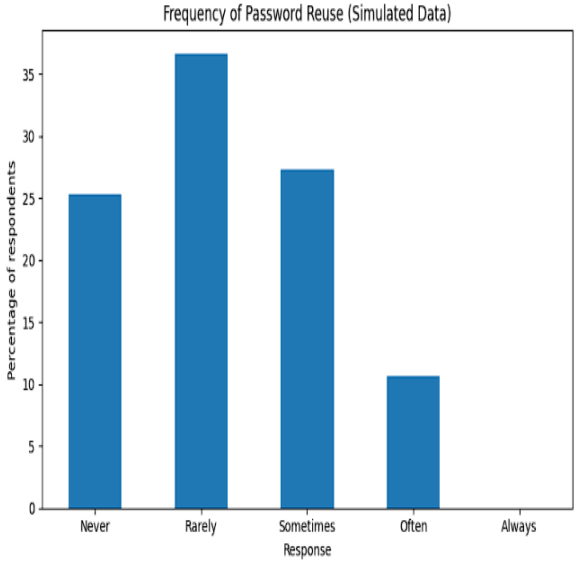
A Chi-Square test was also used to evaluate the association between the identification of the safe password and frequent reuse of passwords. The relationship was not found to be statistically significant ($\chi^2 = 0.258$, $p = 0.612$) in the simulated data.

In summary, it may be said that the simulated analysis displayed the type of knowledge-behaviour gap explored by this study. In particular, the analysis displayed that the general recognition of secure password practices and knowledge of the safest password did not necessarily translate into secure practices.

V. GRAPHICAL ANALYSIS

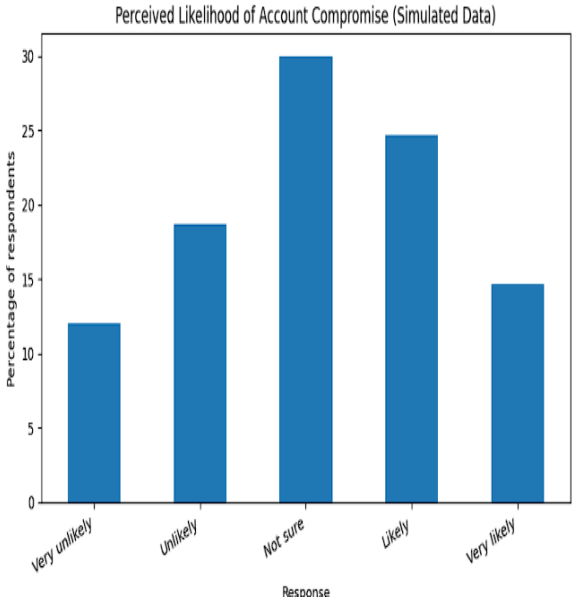
The following graphs are used to present the main patterns:

Figure 1. Frequency of Password Reuse



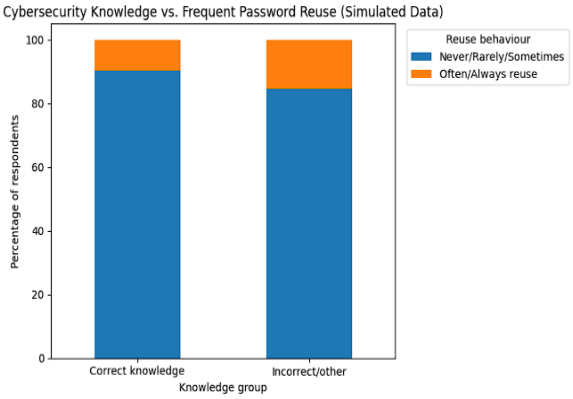
Shows the distribution of respondents according to how frequently they reuse passwords.

Figure 2. Perceived Likelihood of Account Compromise



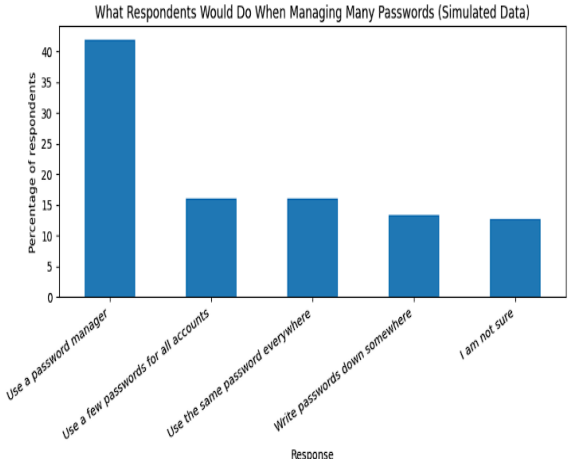
Shows respondents' perception of their vulnerability to password-related account compromise.

Figure 3. Cybersecurity Knowledge vs. Frequent Password Reuse



Compares respondents who correctly identified a secure password with their reported password-reuse behaviour.

Figure 4. Password Management and Convenience



Shows how respondents would manage multiple passwords when remembering separate passwords becomes difficult.

VI. CONCLUSION

The Password Behaviour Paradox shows a gap between what people know about cybersecurity and how they actually act with passwords. Studies show that users know why strong unique passwords matter. Users still reuse passwords or pick simple passwords [1][6]. This means that knowing about cybersecurity is not enough to explain why users act insecurely with passwords.

Research also shows that what users see as risk and how convenient password use is can shape users' choices. Users may see the danger of passwords but

the work needed to remember many passwords push users toward easier options. So, password security behaviour is shaped by what users know what risk users. How users juggle security with convenience [1][2][4].

These findings matter for colleges and universities. Cybersecurity education should do more than give rules; it should also solve the problems students have with account management. Encouraging password managers using multi-factor authentication and teaching real-world password habits can lower these barriers. Help students keep safer passwords. I am convinced that these steps can make a difference.

This study has limits because of its design and because people reported what they think they do. The answers may not match what users actually do with passwords. The design cannot prove cause and effect. Future research could address these limits by using more varied groups following users over time and studying how password habits change.

In short making passwords safer needs more, than telling people what to do. Looking at how cybersecurity knowledge, perceived risk, convenience and password behaviour interact can explain why users know the choice but do not always follow it.

VII. LIMITATIONS

Self-Report Bias: The study uses self-reported information, which may not accurately represent participants' actual password practices. Respondents may give inconsistent answers to questions about password reuse.

Convenience Sampling: The study utilizes a convenience sample, which may not be representative of the larger student population or target population.

Limited Sample Population: The study is conducted among university students who are 18 years of age or older; the results may not be generalizable to other populations and age groups.

Cross-Sectional Design: The study's design is cross-sectional, meaning that data is collected at a specific moment in time. As such, the study cannot establish causation or temporal relationships between observed variables.

Account Context: The study's questionnaire does not differentiate between various online accounts. Practically, respondents may use different security mechanisms for different accounts depending on the account's level of sensitivity and importance.

Limited Number of Variables: The study focuses on cybersecurity knowledge, perceived risk, convenience, and password behavior. However, there are several other factors that impact password behavior, including digital literacy levels, experience with security breaches, the use of password managers, and other organizational factors.

Online Survey Limitations: Since the study's questionnaire is distributed online, it may fail to reach respondents who do not engage with digital communication methods actively.

REFERENCES

[1] Merdenyan, B., and H. Petrie, "Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours," Behaviour & Information Technology, vol. 41, no. 12, pp. 2514–2527, 2022, doi: 10.1080/0144929X.2021.2019832.

[2] Zhang, L., and W. C. McDowell, "Am I really at risk? Determinants of online users' intentions to use strong passwords," Journal of Internet Commerce, vol. 8, nos. 3–4, pp. 180–197, 2009, doi: 10.1080/15332860903467508.

[3] Antony, A., "Study on user compliance with password guidelines using Protection Motivation Theory," Preprint, 2024, doi: 10.13140/RG.2.2.14805.64486.

[4] Duggan, G. B., H. Johnson, and B. Grawemeyer, "Rational security: Modelling everyday password use," International Journal of Human-Computer Studies, vol. 70, no. 6, pp. 415–431, 2012, doi: 10.1016/j.ijhcs.2012.02.008.

[5] Furnell, S., "Assessing website password practices—unchanged after fifteen years?" Computers & Security, vol. 120, Art. no. 102790, 2022, doi: 10.1016/j.cose.2022.102790.

[6] Alqahtani, M. A., "Factors affecting cybersecurity awareness among university students," Applied Sciences, vol. 12, no. 5, Art. no. 2589, 2022, doi: 10.3390/app12052589.

[7] Sivakumar, S., and S. Venkataraman, "Cracks in digital defense: A study on password security awareness and behavior in college

students," ICTACT Journal on Soft Computing, vol. 16, no. 3, 2025, doi: 10.21917/ijsc.2025.0557.

[8] Kumar, A., and P. Nanda, "Cyber safe or cyber risk? An assessment of student practises in password security, phishing and social engineering," Preprint, 2026, doi: 10.36227/techrxiv.177015935.56095390.

[9] Shen, C., T. Yu, H. Xu, G. Yang, and X. Guan, "User practice in password security: An empirical study of real-life passwords in the wild," Computers & Security, vol. 61, pp. 130–141, 2016, doi: 10.1016/j.cose.2016.05.007.

[10] Awad, M., Z. Al-Qudah, S. Idwan, and A. H. Jallad, "Evaluating password behavior at a small university," Journal of Computer Science, vol. 15, no. 1, pp. 1–9, 2019, doi: 10.3844/jcssp.2019.1.9.