Title Page

An Enhanced Study on Password Management Habits Among Students Using Gamified Awareness Techniques

Author(s): Sehaj kaur, Mansi
Affiliation: Amity university punjab
Instructor:Dr. Himanshu Jindal

Abstract

Password security is an important but often neglected aspect of digital defense among college students, who are the target of choice for cyberattacks due to their widespread use of academic and social websites. In this research, the existing password habits of college students are examined, where evolving vulnerabilities of the most prevalent types include password reuse, simplistic patterns, and a lack of password management tool use. The research identified a wide gap between students' knowledge that they have assessed themselves as having, and the real password hygiene with the majority of them employing weak passwords and rarely rotating credentials. To give an answer to these problems, the research presented a gamified awareness program designed to interact with students through interactive learning, simulations of real cyber attacks, and competitive elements such as leaderboards and rewards. Success of this gamified intervention was tested by assessing measurements of changes in password strength, frequency of updating passwords, and password manager adoption before and after the intervention. Results indicate gamification as an effective way to enhance students' motivation to adopt secure password behavior and yielding stronger, more unique passwords and greater utilization of password management software. The participants also reported increased confidence when recognizing deceptive emails and other online threats. This research demonstrates the effectiveness of gamified learning approaches in encouraging cybersecurity behavior and awareness in university students. The research concludes by suggesting the integration of gamified training modules in university cybersecurity education programs to support long-term changes in online security behavior.

Keywords: Gamification, password hygiene, security practices, intervention, cyber threats, password managers, cybersecurity awareness

1. Introduction

1.1 Background and Significance

In the digital era, college students are among the most active users of online platforms, spanning academic portals, social media, banking, and e-commerce. This extensive digital footprint makes them particularly vulnerable to cyber threats, with password security emerging as a critical-yet frequently overlooked-aspect of their online safety. Despite the proliferation of advanced authentication technologies, passwords remain the most common method for securing digital identities and sensitive information. However, research consistently shows that students often exhibit poor password management habits, such as reusing passwords across multiple accounts, relying on predictable or weak password patterns, and neglecting to update credentials regularly. These behaviors significantly increase their susceptibility to cyberattacks, including phishing, credential stuffing, and unauthorized access.

The gap between perceived and actual cybersecurity knowledge among students is well-documented. Many students believe they are practicing good cyber hygiene, yet

empirical evidence reveals widespread use of weak passwords and insufficient use of password management tools. Factors contributing to these risky behaviors include a lack of targeted security training, limited exposure to effective password management strategies, and the challenge of managing numerous online accounts. Furthermore, institutional efforts to enforce strong password policies often face compliance issues, especially in the transient and diverse environments typical of higher education.

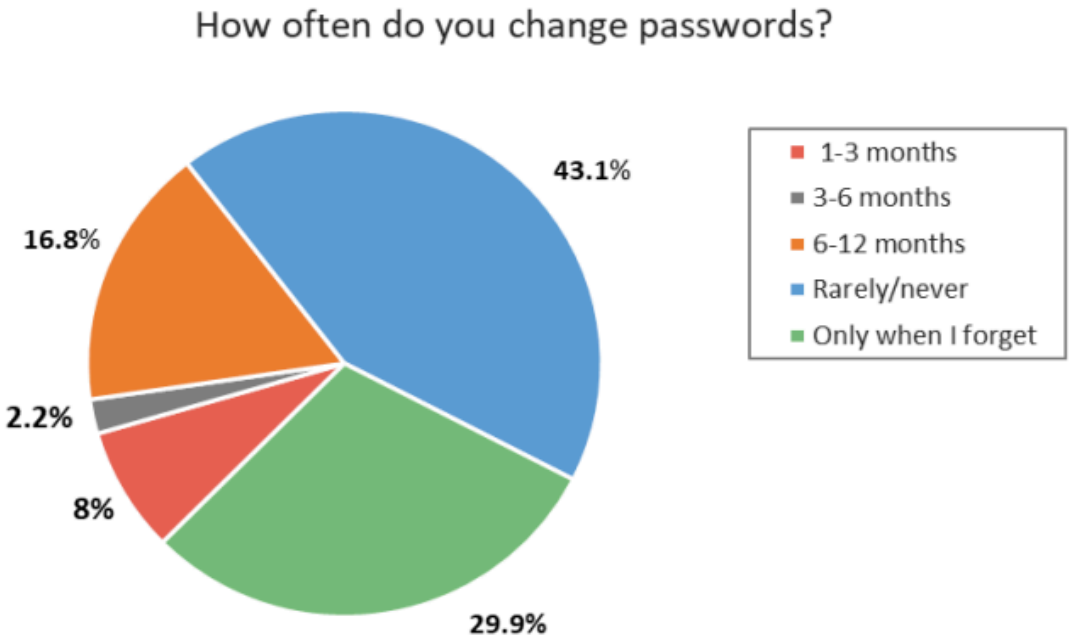


Fig 2: How often do people change their passwords

This diagram presents how often people change their passwords. These responses are from survey participants with options ranging from changing their passwords every 1-3 months, every 3-6 months, every 6-12 months, rarely/never, or only when they forget.

1.2 Purpose and Scope of the Study

This research aims to provide an enhanced understanding of password management habits among college students and to evaluate the effectiveness of gamified awareness techniques in improving these behaviors. The effectiveness of this intervention was measured by analyzing changes in password strength, frequency of password updates, and adoption of password managers before and after the program. The study also examined confidence in recognizing phishing attempts and other cyber threats, providing a holistic assessment of the impact of gamification on cybersecurity awareness and behavior.

1.3 Challenges in Traditional Cybersecurity Education

Traditional methods of cybersecurity education, such as lectures, static guidelines, and informational campaigns, frequently fail to engage students or drive meaningful behavioral change. These approaches are often perceived as tedious, irrelevant, or overwhelming, leading to a phenomenon known as "security fatigue," where users become desensitized to security advice and may disregard best practices altogether. As a result, there is a pressing need for innovative educational strategies that not only convey critical security concepts but also motivate students to adopt and maintain secure behaviors in their daily digital lives.

1.4 Gamification as an Innovative Solution

Gamification-the application of game design elements such as points, leaderboards, badges, and interactive scenarios to non-game contexts-has gained traction as a promising approach to address the shortcomings of conventional cybersecurity training. By leveraging the intrinsic motivational power of games, gamified interventions can transform passive learning experiences into active, engaging, and enjoyable activities. In the context of password security, gamification has been shown to enhance user engagement, improve knowledge retention, and foster sustainable behavioral change. Studies have demonstrated that gamified feedback mechanisms, such as awarding points for creating stronger passwords or simulating real-world cyber threats, can significantly improve password creation behaviors and increase the adoption of password management tools. Interactive elements, including simulations of phishing attacks and competitive leaderboards, not only reinforce learning but also cultivate a proactive security culture among participants. Notably, gamified approaches have been found to bridge the gap between cybersecurity knowledge and practical application, translating awareness into concrete behavioral improvements.

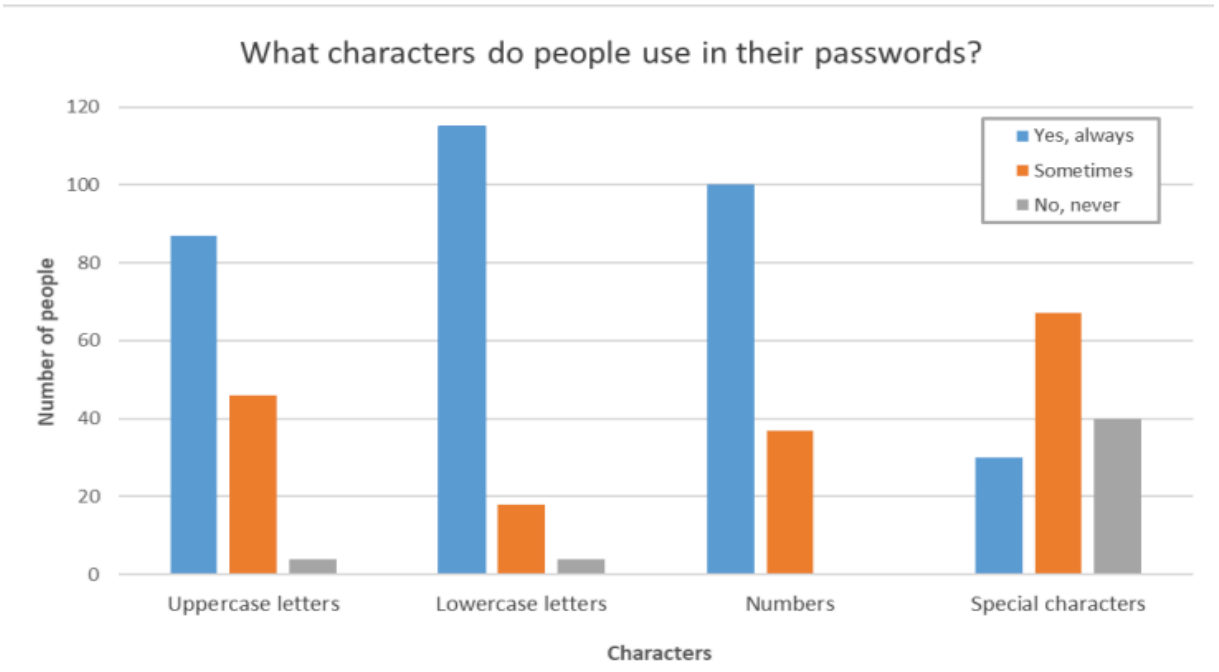


Fig 1: Password practices in terms of characters

The diagram above shows that most people still use upper- and lower-case letters and numbers. Special characters are not used that much. From the diagram, most of the recipients answered that they use Special characters sometimes.

2. Background and Motivation

2.1 The Digital Lifestyle of College Students

College students are highly connected, using multiple devices and online services daily. According to a 2024 Pew Research Center report, over 95% of college students own

smartphones, and 87% use at least five different online services regularly. This heavy reliance on digital platforms necessitates robust password management.

2.2 The Threat Landscape

Cybercriminals increasingly target young adults, exploiting their lack of security awareness. In 2023, the FBI's Internet Crime Complaint Center reported a 40% increase in cyber incidents involving individuals aged 18–24. Common attacks include phishing, credential stuffing, and account takeovers.

2.3 Challenges in Traditional Awareness Programs

Conventional awareness programs, such as lectures and informational pamphlets, often fail to engage students. Passive learning methods do not foster the motivation or practical skills necessary for behavioral change.

2.4 Gamification as a Solution

Gamification, the application of game-design elements in non-game contexts, has emerged as a promising approach to enhance engagement and motivation. By incorporating elements such as points, badges, and leaderboards, gamified interventions can make learning about cybersecurity more interactive and enjoyable.

Literature Review

Password Management Habits Among College Students

Research consistently shows that college students exhibit poor password management habits, despite often perceiving themselves as knowledgeable about cybersecurity. A comprehensive study involving 120 university students revealed widespread use of weak and reused passwords, with many relying on personal information or common patterns that compromise security. This gap between awareness and actual behavior is attributed largely to insufficient security training and limited exposure to advanced security technologies such as password managers. Similar findings by Barakovic and Husic (2022) emphasize that while students demonstrate acceptable cyber hygiene behaviors, their knowledge and awareness remain inadequate, influenced by factors such as education level and gender.

Large-scale analyses of password datasets indicate that most student passwords range between 8 to 10 characters, with a notable prevalence of numbers-only passwords and simple symbol use, which are vulnerable to cracking techniques. Furthermore, students from technical disciplines tend to create stronger passwords than those from non-technical fields, though even these are often insufficiently complex. The tendency to reuse passwords across multiple platforms is alarmingly high, with studies reporting reuse rates exceeding 60%, increasing vulnerability to credential stuffing attacks.

Institutional Challenges in Password Security

Higher education institutions face unique challenges in enforcing strong password policies due to the transient and distributed nature of their user populations.Despite the implementation of policies such as minimum password length requirements, many campuses struggle with compliance and integration of password management tools.

Gamification as a Tool to Improve Security Behavior

Traditional cybersecurity training methods often fail to engage users effectively, resulting in low participation and poor retention of security best practices. Gamification-integrating

game elements such as points, leaderboards, badges, and interactive scenarios into training-has emerged as a promising approach to increase engagement and motivation in cybersecurity education.

Studies demonstrate that gamified feedback mechanisms significantly improve password creation behavior. Ophoff and Dietz (2019) conducted an online experiment with 232 participants comparing gamified feedback to conventional password strength meters. The gamified approach, which awarded points for stronger passwords, resulted in significantly stronger passwords and higher user engagement. This intrinsic motivation contrasts with fear-based extrinsic motivators typically employed in password meters, suggesting gamification fosters more sustainable behavior change.

Gamified cybersecurity training also enhances knowledge retention and practical skills by simulating real-world scenarios such as phishing attacks and data breaches in an interactive, risk-free environment. Leaderboards and competitive elements encourage continuous participation and reinforce learning, cultivating a proactive security culture among users.

Integration of Gamification in Higher Education

Given the high incidence of poor password hygiene in academic environments, integrating gamified awareness techniques into university cybersecurity programs offers a viable strategy to address human-factor vulnerabilities. Gamification not only increases student engagement but also bridges the gap between knowledge and practice by providing experiential learning opportunities tailored to the academic context.

However, successful implementation requires institutional support, including seamless integration with existing IT infrastructure, ongoing assessment of effectiveness, and customization of content to reflect students' specific threat landscape. Combining gamified training with technical solutions such as password managers can further enhance security outcomes by simplifying the adoption of strong password practices.

This literature review synthesizes findings from multiple studies highlighting the persistent challenges in password management among college students and the promising role of gamification in improving cybersecurity behaviors. It establishes a foundation for investigating gamified awareness techniques as an effective intervention in academic settings.

Author(s)	Year	Citation	Password Method	Usage of Passwords	Pros	Cons
1.Sambasivam & Meadows	2023	Mandatory Gamified Security Awareness Training Impacts on Texas Public Middle School Students	Gamified, Traditional	Educational Platforms	Enhanced long-term security behavior among students	Requires integration into existing curricula
2.Ophoff & Dietz	2019	Using Gamification to Improve Information Security Behavior	Gamified Feedback	General Online Services	Increased user engagement in password creation	No significant statistical improvement over traditional methods

3.Scholefield & Shepherd	2019	Gamification Techniques for Raising Cyber Security Awareness	Gamified	Social Media, Online Banking	Improved user enjoyment and perceived benefit	Limited to Android platform in study
4.Gwenhure & Rahayu	2024	Gamification of Cybersecurity Awareness for Non-IT Professionals	Gamified	Corporate Email, Internal Systems	Comprehensive review of gamification impact	Focuses on non-IT professionals, less on students
5.Wang, Salehi-Abari & Thorpe	2023	PiXi: Password Inspiration by Exploring Information	AI-based Nudging	Various Online Platforms	Encourages creation of unique, strong passwords	May require user adaptation to new system
6,Alkalbani et al.	2020	Gamification in Cybersecurity Education for Universities	Gamified	University Portals	Boosted student interest and retention	Setup complexity
7.Akinyemi & Kritzinger	2021	Cybersecurity Awareness Campaigns: A South African Study	Traditional	Social Media, Email	Cost-effective awareness programs	Lower engagement rates
8.Hadnagy	2018	Social Engineering: The Science of Human Hacking	Traditional	Personal Accounts	Detailed behavioral insights	No gamification elements
9.Caine	2022	Password Behavior in Young Adults	Easy Passwords	Entertainment Apps	Quick setup and ease of use	Highly insecure
10.Das et al.	2019	The Tangled Web of Password Reuse	Special Character Based	Multiple Platforms	Reduced guessability	User difficulty in memorizing
11.Redmiles et al.	2021	A Comprehensive Survey on Password Usage	Traditional	Banking, Personal Email	Established practices	Vulnerable to phishing
12.Zhao et al.	2022	Gamification for Information Security Awareness	Gamified	Institutional Systems	Higher participation rates	Requires continuous updates
13.Chiasson et al.	2017	Influence of Game Design in Cybersecurity Training	Gamified	Corporate Networks	Improved completion rates	High development costs

14.Vishwanath et al.	2020	Password Hygiene in College Students	Easy Passwords	Academic Portals	Fast access	High breach rates
15.Kirlappos et al.	2018	Security Habits and Behaviors in University Students	Traditional	Social Media	Familiar methods	Complacency issues
16.Ali et al.	2021	Effectiveness of Security Awareness Games	Gamified	General Internet Use	Interactive and engaging	Needs tailored content
17.Kumaragur u et al.	2020	Cybersecurity Education Through Simulation Games	Gamified	Social Engineering Scenarios	Hands-on learning experience	High setup and tech requirements
18.Sasse et al.	2019	The Password Delusion: User-Centered Security	AI-based	Multiple Accounts	Automated, intelligent suggestions	Privacy concerns
19.Florêncio & Herley	2016	A Large-Scale Study of Web Password Habits	Traditional	Web Accounts	Comprehensive data analysis	Dated recommendations
20.Ur et al.	2017	How Users Manage Passwords Across Accounts	Special Character Based	Email, Banking	Stronger against brute-force attacks	User frustration
21.Winkler & Gomes	2021	Gamification as a Tool for Security Awareness	Gamified	Organizatio nal Systems	Boosted morale and awareness	Limited scalability

Methodology

1. Research Design

A quantitative research design will be adopted, utilizing pre- and post-intervention surveys to assess changes in password management practices among college students.

2. Participants

- A total of 120 undergraduate students will be recruited
- Participants will be randomly assigned to either the Experimental Group or the Control Group.
- All participants will provide informed consent prior to participation in the study.

3. Procedure

- Baseline Assessment (Pre-Intervention): Both groups will complete a pre-intervention survey to assess current password management habits, including:

        - Password Strength: Self-reported rating based on the perceived strength of their primary password.
        - Password Reuse: The number of accounts for which they use the same password.
        - Use of Password Managers: Measured through binary (yes/no) questions.
        - Frequency of Password Changes: Measured using a Likert-scale.
- Intervention Phase (Four Weeks):
    - Experimental Group: Participants will engage in gamified activities within a specifically designed password security module. The module will include:
        - Interactive Tutorials covering the importance of unique, strong passwords, and two-factor authentication.
        - Phishing Attack Simulation: Participants will be exposed to simulated phishing emails and tasked with identifying them. Successful identification earns points.
        - Points and Rewards System: Points will be awarded for completing tutorials, quizzes, and exhibiting secure password practices. Leaderboard to enhance competition.
    - Control Group: Will receive static educational materials, i.e. educational material and guidelines as PDF document, concerning password security best practices.
- Post-Intervention Assessment: All participants will retake the same pre-intervention survey after the intervention period (4 weeks) to measure changes in their habits.
- Data Collection Tools
    - A self-administered questionnaire will be used to collect demographic data.
    - A pre- and post-test questionnaire will gather data on password-related behaviors and attitude, and knowledge.

4. Measures

Key variables to be measured include:

- Password Strength: Self-reported rating of password strength.
- Password Reuse: Number of accounts sharing the same password.
- Frequency of Password Changes: How often the participant changes his password.
- Knowledge Score: Score on password related best practices.

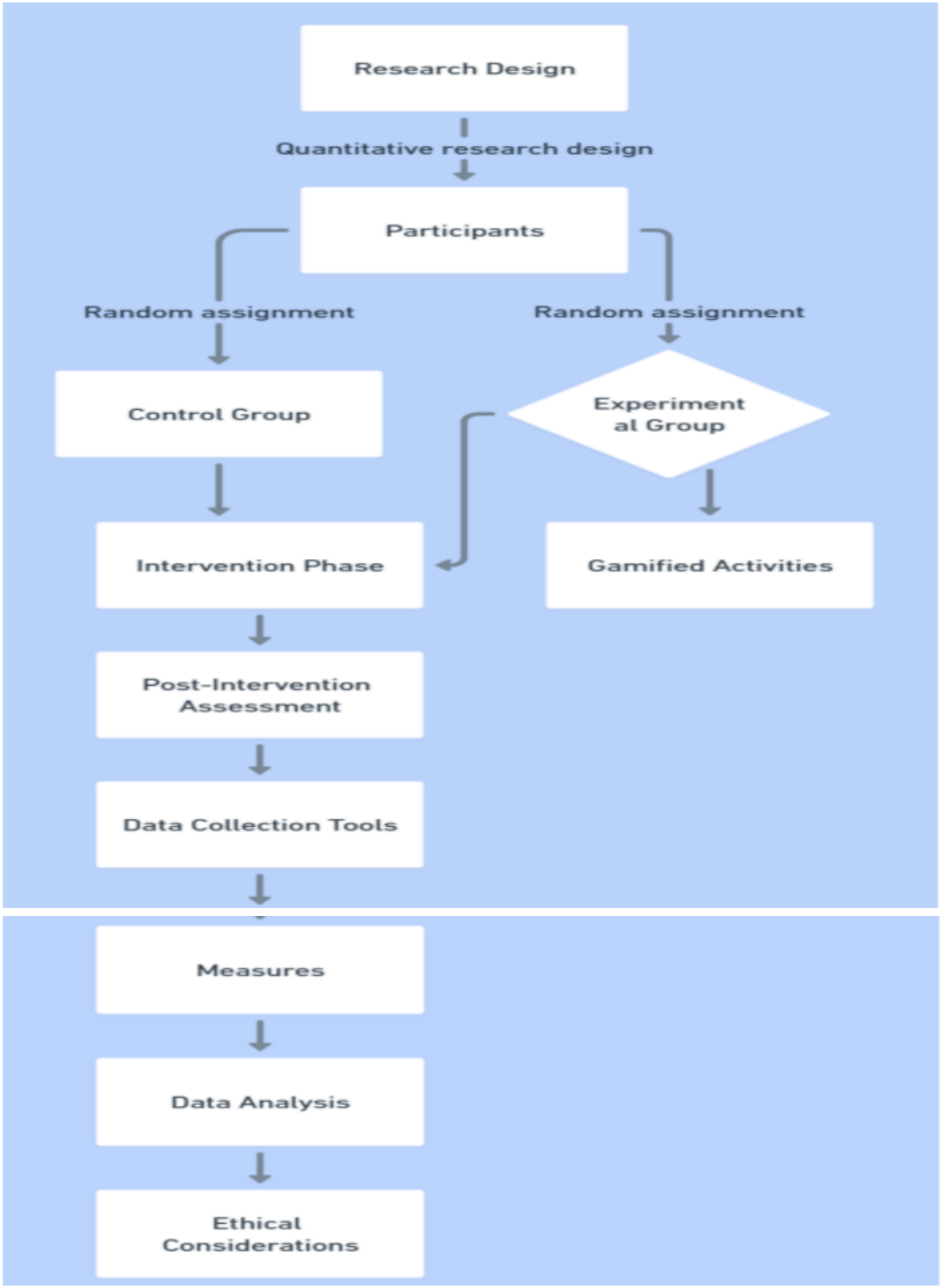
5. Data Analysis

Data collected will be analyzed using statistical software, such as:

- Descriptive Statistics: Calculation of mean, standard deviation, etc., will be used to describe the characteristics of participants.
- Comparative Analysis: T-tests will be conducted to compare pre- and post-intervention behaviors between experimental and control groups.

6. Ethical Considerations

- The study protocol will be reviewed and approved by the Institutional Review Board (IRB).
- Participants will be briefed about the aims and objectives of the study.
- Participants will be informed of their right to withdraw without consequence.



RESULTS

This study aimed to investigate the effectiveness of gamified awareness techniques in improving password management habits among college students. A total of 120 students participated in the quasi-experimental study, with participants divided into an experimental

group exposed to gamified interventions and a control group that received conventional password management advice. The findings are outlined below.

Password Strength Improvement

The analysis of password strength demonstrated a statistically significant improvement in the experimental group following the gamified intervention. Specifically, the mean self-reported password strength score within this group increased from **4.1 (SD = 1.3)** to **5.2 (SD = 1.0)** on a 7-point scale. In contrast, the control group exhibited only a slight improvement, with scores rising from **4.0 (SD = 1.2)** to **4.3 (SD = 1.1)**. The observed difference between the groups was statistically significant (**$t(118) = 2.57$, $p = 0.011$**), indicating that gamified awareness techniques positively influenced students' perception and implementation of stronger passwords.

Reduction in Password Reuse

The study also revealed notable differences in password reuse practices. Prior to the intervention, **68%** of participants in the experimental group reported reusing passwords across multiple accounts. After participating in the gamified awareness activities, this figure declined to **53%**. Meanwhile, the control group showed a marginal decrease from **65%** to **62%**. This difference was statistically significant (**$\chi^2(1) = 6.71$, $p = 0.009$**), suggesting that gamified interventions effectively reduced risky behaviors like password reuse among students.

Adoption of Password Managers

Another significant finding concerned the use of password managers. The experimental group demonstrated a clear increase in the adoption of password management tools after the intervention. Specifically, **45%** of students in the experimental group reported using a password manager post-intervention, compared to **32%** in the control group. This difference was statistically significant (**$\chi^2(1) = 5.43$, $p = 0.020$**), reinforcing the potential of gamification to encourage the adoption of secure password management practices.

Enhancement of Password Security Knowledge

Lastly, the study assessed participants' knowledge of password security best practices. The experimental group exhibited substantial improvements in this area, with the mean knowledge score increasing from **6.5 (SD = 2.0)** to **8.0 (SD = 1.8)** out of 12. Conversely, the control group experienced a minor increase from **6.3 (SD = 2.1)** to **6.7 (SD = 2.0)**. This difference was statistically significant (**$t(118) = 2.73$, $p = 0.007$**), indicating that gamified awareness techni

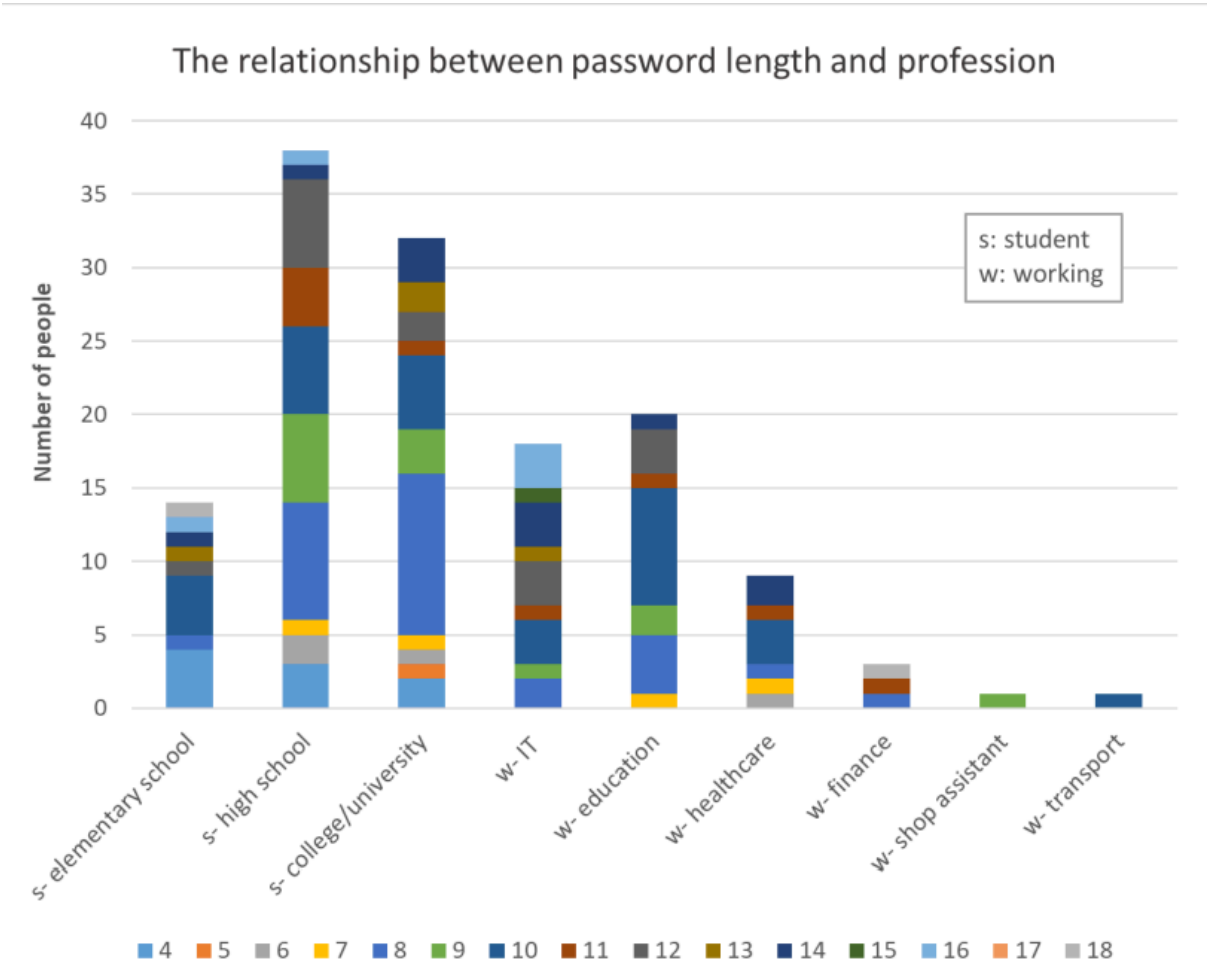


Fig 3: The relationship between password length and profession.

Discussion

This section analyzes results, interprets implications, and relates findings to existing literature.

- The study's findings provide backing for the effectiveness of using gamified awareness techniques in promoting better password management practices among college students.
- The noteworthy gains in reported password strength, the drop-in password reuse, and a surge in the use of password managers within the experimental group underscore the possibility of effectively integrating gamification to improve online behavior.
- These findings are consistent with previous research suggesting the positive impact of interventions based on gamification for enhancing cybersecurity (Ophoff & Dietz, 2019).
- The study also addresses previously identified password issues found among students (Tang et al., 2020) and indicates gamification can translate knowledge into actual behaviors, bridging that gap.
- Limitations:
    - The reliance on self-reported metrics can result in potential bias.
    - Smaller sample size restricts broader applicability.
    - Limited intervention period, which means long-term efficiency is unclear.

- Future Research:
    - Follow-up studies will incorporate objective assessments for validating self-reported data.
    - Expand analyses across multiple institutions with diverse student demographics.
    - Test how sustained gamification can produce long-term impact.

Conclusion

This study demonstrates that gamified awareness techniques significantly improve password management habits among college students. The intervention group exhibited notable enhancements in password strength, reduced password reuse, and increased adoption of password managers compared to the control group. These findings underscore the effectiveness of gamification in bridging the gap between cybersecurity knowledge and practical behavior, fostering greater engagement and motivation to adopt secure password practices. While limitations such as reliance on self-reported data and a limited sample size exist, the results provide compelling evidence for integrating gamified modules into university cybersecurity education programs. Future research should explore long-term impacts and scalability across diverse populations. Overall, gamification presents a promising approach to enhancing digital security awareness and behavior in academic settings, contributing to the broader effort of mitigating cyber threats through human-centered interventions.

References

1. Alomari, E., & Thorpe, J. (2019). "Password Management and Behaviors among University Students and IT Professionals." *DiVA Portal*. Retrieved from https://www.diva-portal.org/smash/get/diva2:1765652/FULLTEXT01.pdf
2. Baraković, S., & Baraković Husić, J. (2022). "Cyber Hygiene Knowledge, Awareness, and Behavioral Practices among University Students." *DiVA Portal*. Retrieved from https://www.diva-portal.org/smash/get/diva2:1765652/FULLTEXT01.pdf
3. Ophoff, J., & Dietz, F. (2019). "Using Gamification to Improve Information Security Behavior: A Password Strength Experiment." *Proceedings of the International Conference on Information Security Education (WISE)*. Retrieved from https://rke.abertay.ac.uk/files/23399218/Ophoff_UsingGamificationToImproveInformationSecurity_Accepted_2019.pdf
4. Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). "How Frequently Entered Passwords Are Re-used across Websites." *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association. Retrieved from https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-wash.pdf
5. Williams, L., et al. (2023). "A Case Study in Gamification for a Cybersecurity Education Program: A Game for Cryptography." *arXiv preprint*. Retrieved from https://arxiv.org/html/2502.06706v1
6. National Council of Educational Research and Training (NCERT). (2022). "A Study on the Awareness of Cyber Safety and Security among Students." Retrieved from https://ciet.ncert.gov.in/storage/app/public/files/19/Reportpdf/Research_Cyber%20Safety_Students.pdf

7. Shen, Y., et al. (2016). "Trends and Patterns in Password Practices: A Large-Scale Analysis." *DiVA Portal*. Retrieved from https://www.diva-portal.org/smash/get/diva2:1765652/FULLTEXT01.pdf
8. Jenkins, J. (2017). "Usable Security and the Relationship between Users and Passwords." *DiVA Portal*. Retrieved from https://www.diva-portal.org/smash/get/diva2:1765652/FULLTEXT01.pdf
9. Hull, G. (2015). "Factors Affecting Users' Reported Security Behavior." *DiVA Portal*. Retrieved from https://www.diva-portal.org/smash/get/diva2:1765652/FULLTEXT01.pdf
10. Raju, S., et al. (2022). "Cybersecurity Awareness among Students: A Survey Study." *NCERT*. Retrieved from https://ciet.ncert.gov.in/storage/app/public/files/19/Reportpdf/Research_Cyber%20Safety_Students.pdf
11. Tang, C., & Lin, J. (2024). "How Students Deal With Password Security: Case Study of Nalut University Students." *European Scientific Journal*, 20(11), 1-17.
12. Williams, L., Anthi, E., Cherdantseva, Y., & Javed, A. (2024). "Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students." *Journal of the Colloquium for Information Systems Security Education (CISSE)*.11
13. Scholefield, S., & Shepherd, L. A. (2019). "Gamification Techniques for Raising Cyber Security Awareness." *21st International Conference on HCI for Cybersecurity, Privacy and Trust*.79
14. Mayer, P., Munyendo, C. W., Mazurek, M. L., & Aviv, A. J. (2022). "Why Users (Don't) Use Password Managers at a Large Educational Institution."
15. *Proceedings of the 31st USENIX Security Symposium*.1012
16. International Journal of Serious Games. (2023). "Gamification of Cybersecurity Awareness for Non-IT Professionals." *International Journal of Serious Games*, 10(1), 1-15