# \*\*\*Password Complexity and Awareness

In this modern digital era, where authentication is an integral part of almost all the systems, it has become more challenging to keep ourselves protected by a strong password. In general, the strength of the password is determined by the combination of characters, symbols, upper case and lower case, unique numbers and potentially the length of password itself. In good computer security practice, It is very important that the passwords are between eight (8) and twenty-four (24) characters long combined with at least one uppercase letter, one number, and one unique character [1].

However, excessively complex passwords can have a negative impact on user compliance, as they may turn into insecure practices of writing down the passwords or reusing them across multiple platforms [2]. Hence, comprehensive cybersecurity awareness programs are very critical in educating users to inherit secure as well as user friendly password creation techniques such as passphrases and password managers [3]

\*\*Awareness and Training Strategies

An effective awareness and training program for creating secure and user-friendly passwords must be combined with both educational sessions and interactive activities to balance complexity with usability. Following are some of the key strategies to be included in the awareness and training program.

1. Passphrase encouragement: All the users should be encouraged in creating passphrases which are long, memorable phrases that can enhance complexity without sacrificing ease of recall [4].In this strategy, if though the length of password seems long, they are more recallable to user’s mind eventually making the passwords more secure and less prone to hijacking.
2. Interactive Simulations: To identify and respond properly to password related security threats, simulated phishing exercises and practical workshops should be conducted on regular basis [4]. These simulations should realistically mimic common attacks on real time world, leaving immediate feedback to the participants
3. Continuous Reinforcement and Compliance Monitoring: It is best to have regular communication through monthly cybersecurity newsletters, briefings, or reminders on good password habits. Additionally, compliance audits and automatic checks on password strengths through company systems or password auditing tools will help in maintaining user accountability, encouraging adherence, and reducing complacency.
4. Gamification Strategies: Gamification, which is pretty engaging for most of the users, can be an effective strategy to enhance user engagement with cybersecurity practices. Activities like quizzes, leaderboards, badges, and friendly competitions can be the base for training that motivates the employees through recognition and rewards. The principle behind this strategy is it takes advantage of addictive nature of the human brain to create enthusiasm and motivation in relevant and required field [5].

A diagram of steps for implementation

AI-generated content may be incorrect.

***Fig: [6] -Key steps for implementing Gamification***

\*\*\*References

1. Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, *12*(5), 2589. <https://doi.org/10.3390/app12052589>
2. Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016, May). Do users' perceptions of password security match reality?. In *Proceedings of the 2016 CHI conference on human factors in computing systems* (pp. 3748-3760).
3. Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019). Why people (don't) use password managers effectively. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)* (pp. 319-338).
4. Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. International Journal of Human-Computer Studies, 131, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005
5. Holdsworth, Jack & Apeh, Edward. (2017). An Effective Immersive Cyber Security Awareness Learning Platform for Businesses in the Hospitality Sector. 111-117. 10.1109/REW.2017.47.
6. HiFives (2022). *Gamification as a Means of Enhancing Employee Engagement*. [online] Employee Rewards, Recognition & Engagement Platform. Available at: https://www.hifives.in/gamification-as-a-means-of-enhancing-employee-engagement/ [Accessed 23 Jul. 2025].