No Rules: Can Removing Password Creation Rules Improve Password Memorability and Security?

Naomi Woods
University of Jyväskylä, Finland

naomi.woods@jyu.fi

Abstract: Many users have significant issues in remembering all their passwords. There are several authentication technologies available on the market to help with these issues, for instance, password managers. However, many users still choose to rely solely on their memory. Creating and recalling multiple strong passwords often leads many users to adopt insecure password practices, such as, creating weak passwords and writing passwords down. Insecure behaviours result in substantial security breaches and financial losses. Therefore, password creation requirements imposing complexity (e.g., X number of higher and lower case letters, numbers and special characters), and length (e.g., X number of characters) are implemented to ensure that users create passwords with a standard or minimum level of strength. Previous research has examined password memory and security issues, suggesting various ways to improve memorability. Furthermore, previous research has also examined users' perceptions and interactions when attempting to meet password creation requirements, and the impact they have on users' password management. Previous results suggest that users struggle to meet password creation rules and often circumvent security by, for instance, reusing the same password or modifying passwords for multiple accounts, which is a significant security issue unto itself. In this study, we will examine whether removing the complexity password creation rules will have beneficial effects on memorability and security. Using a mixed-method study, we will examine password creation and recall, using an online laboratory study, observing the strength of the passwords, and whether focusing solely on creating and not meeting rules will improve password memorability. Follow-up questionnaires will measure user perceptions and attitudes, and interviews will be conducted to deeper examine motivations for digital security while not imposing rules. The results will have important implications for research and practice, and especially for professionals who make recommendations and guidance for password management. This is because, improving password memorability and security could reduce insecure password behaviours and reduce financial losses associated with passwords.

Keywords: Passwords, Password creation requirements, Password behaviour, Memorability, Authentication

1. Introduction

Passwords are the most common authentication mechanism. Even with several security issues pertaining to them, they remain prevalent due to their low cost and how easily they are implemented into systems (Bošnjak & Brumen 2019; Güven et al., 2022; Wang et al. 2025). Over recent years, with a significant increase in digital accounts, users are now expected to have on average, over 100 passwords (Woods & Siponen 2025). Multiple password usage is leading many users to struggle as they attempt to create strong and easy to remember passwords, of which they then often adopt insecure password behaviours such as writing passwords down and reusing passwords to cope with these issues (Das et al., 2014; Woods & Siponen, 2018; 2025; Zimmermann and Gerber, 2020). These insecure behaviours are leading to substantial security breaches, with organizations losing hundreds of thousands of dollars per breach (Merdenyan & Petrie, 2022; Woods & Siponen 2025). In response to the password problem, new authentication solutions have entered the market, including password managers to help keep passwords secure, and multifactor authentication (MFA) solutions to add additional security factors to the authentication process (Daffalla et al. 2025; Das et al. 2019). Yet, passwords are still preferred by many users, and therefore researchers attempt to provide ways to improve the users' password security behaviour, and password memorability (Bošnjak & Brumen 2019; Güven et al., 2022; Siddique et al. 2017).

This paper proposes a study, applying an interdisciplinary approach and drawing upon psychology and cybersecurity to understand how password creation rules affect password memorability and security. It highlights how imposing password rules may be counterintuitive, and examines users' security motivations and implications if users were allowed to be autonomous.

In this proposed study, we suggest that removing complex password creation rules will not only improve password memorability but may also improve their overall security, and will aim to answer these research questions: to what extent does removing password creation requirements improve password memorability? Do users create strong passwords with password creation requirements removed?

2. Password Memorability, Security and Imposing Password Creation Policies

Previous research examining the password problem has often focused on how human memory shapes password related behaviour. Studies have explored factors that influence memorability (e.g., Woods & Siponen, 2018;

2025), the role of perceived importance of information in password creation (Grawemeyer & Johnson, 2011), the impact of password policies on user choices (Campbell et al., 2011; Rodriguez et al., 2022; Shay et al., 2016), and broader patterns in password security practices. Many studies have explored how to improve password memorability by drawing on what is known about human memory — how people learn, store, and retrieve information. This work has been applied across the full password lifecycle, including how users create, learn, and recall passwords, as well as how memory techniques or technological aids might support these stages (e.g., Woods & Siponen, 2018; 2019).

There are two facets of password security, which are interrelated. The first being that users should create strong passwords, by following password creation policies. These password policies are based on NIST SP 800–63 guidelines, to impose a minimal level of strength (minimum number of characters, upper and lower characters, numbers, special characters, etc.) (Campbell et al., 2011; Güven et al., 2022; Rodriguez et al., 2022; Shay et al., 2016). Although these policies have been updated in NIST SP 800–63B (Grassi et al., 2024), with no requirements for complexity; older policies requiring complexity are still imposed on many popular websites and within organizations (Woods & Siponen, 2025). The second facet of password security is the users' behaviour with respect to managing their passwords. Struggling with password memorability can lead to insecure behaviours including reusing and modifying passwords (Grawemeyer & Johnson, 2011; Merdenyan & Petrie, 2022). Many users reuse their passwords, as they believe that it will help them remember their multiple passwords (Das et al., 2014; Zimmermann and Gerber, 2020). When users are prevented from reusing passwords due to varying password policies, they often resort to predictable patterns or small modifications to their existing passwords (Das et al., 2014; Woods & Siponen, 2025). Research suggests that many users believe these minor changes enhance their security, without realizing that such patterns are easily exploitable (Das et al., 2014; Merdenyan & Petrie, 2022).

The purpose of password policies are to encourage users to increase their password strength, with users being required to find the time and mental energy to create and learn passwords that comply with these policies (Marquardson, 2012; Woods & Siponen, 2019). However, human memory has limitations in learning, which are not taken into account in the password creation process, as security policies encourage users to create longer and longer passwords to increase security (Campbell et al., 2011; Marquardson, 2012; Woods & Siponen, 2019). Often, users face the trade-off between password memorability and security due to password composition policies, which results in users choosing to meet the bare minimum due to these constraints (Bošnjak & Brumen 2019; Marquardson, 2012).

3. Rules vs. no Rules: Study Motivation

Technology has been developed that eliminates the need to memorize and recall passwords. One example is, password manager technology which appears to offer a strong solution to the challenges of password memorability and security (Bošnjak & Brumen 2019; Merdenyan & Petrie, 2022). However, they have not achieved widespread adoption despite being available for decades. Research suggests that many users still prefer to memorize their passwords rather than rely on a password manager, and even when encouraged to adopt one, a significant number continue to resist (Das et al., 2014; Wang et al., 2025; Woods & Siponen 2025). Because users largely want to retain personal responsibility for remembering their passwords, finding ways to improve password creation and recall remains essential (Bošnjak & Brumen 2019; Siddique et al. 2017).

During a pilot password study, participants were required to create and recall passwords that met typical password creation policy requirements. The initial results suggested that users were focusing on meeting the password creation rules and not on learning their passwords, which in turn affected their memorability. Therefore, in the proposed study, we will examine whether removing the complexity password creation requirements will have positive effects on memorability as well as overall security, as users will be able to focus on the learning process.

4. Proposed Research Methods: Mixed Method Study

Using a mixed-method approach, we will examine password creation and recall, using a longitudinal online laboratory study (Woods & Siponen, 2018; 2025). Over 200 participants will be recruited from various organizations where several systems and services require password authentication. The participants will be allocated into two groups and will create and recall multiple passwords over several weeks through an online password system, specifically designed for this study. One group will create passwords with password creation rules imposed that include complexity and length requirements, and the second group will have only length requirements imposed while creating their passwords. Password memorability will be measured between both

groups. Additionally, strength will be observed and measured using zxcvbn (a heuristic-based password strength estimator) (Kagnici et al. 2025), to examine whether participants will create complex and long passwords without the requirements in place. Follow-up questionnaires will measure user perceptions and attitudes towards their experience of creating and recalling passwords that meet password creation requirements, and further interviews will be conducted to deeper examine motivations for digital security while not imposing rules.

Ethical approval will be obtained from the institution's ethics committee, and all ethical considerations will be fully observed. Participants will provide informed consent, receive clear information about the study and its privacy practices, and all collected data will be coded and kept confidential.

5. Conclusion

Many users experience persistent difficulty remembering the numerous passwords required across their accounts (Woods & Siponen, 2025). Although a range of authentication technologies has been developed to try to mitigate these challenges, a substantial proportion of users choose to continue to rely exclusively on their own memory (Das et al., 2014; Wang et al. 2025). The demands of creating and recalling multiple strong passwords frequently lead to insecure practices, including the use of weak passwords and writing them down. Such behaviours contribute to significant security incidents and financial losses (Woods & Siponen, 2018). In response, stricter password policies are imposed, with organisations commonly enforcing password creation policies that mandate increased complexity and increased length to ensure password strength. However, these policies can have the opposite effect as users' memories are limited, resulting in a trade-off between password memorability and security (Bošnjak & Brumen 2019; Campbell et al., 2011; Rodriguez et al., 2022; Shay et al., 2016). Therefore, this study proposes examining the effects of removing password complexity requirements on memorability and security to understand whether focusing solely on creating and not meeting rules will improve password memorability.

The findings are expected to offer meaningful implications for both research and professional practice, particularly for those responsible for developing password management guidance. Enhancing the memorability and security of passwords has the potential to reduce insecure user behaviours and, in turn, lessen the financial losses associated with password related security incidents.

Ethics Declaration: Ethical clearance from the institution's ethical committee will be obtained before the study commences.

AI Declaration: AI tools were not used in the development of this paper.

References

Bošnjak, L., & Brumen, B. (2019). Rejecting the death of passwords: Advice for the future. *Computer Science and Information Systems*, *16*(1), 313-332.

Campbell, J., Ma, W., & Kleeman, D. (2011). Impact of restrictive composition policy on user password choices. *Behaviour & Information Technology*, *30*(3), 379-388.

Daffalla, A., Bhattacharya, A., Wilder, J., Chatterjee, R., Dell, N., Bellini, R., & Ristenpart, T. (2025). A framework for abusability analysis: The case of passkeys in interpersonal threat models. In *34th USENIX Security Symposium (USENIX Security 25)* (pp. 7819-7838).

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014, February). The tangled web of password reuse. In *Ndss* (Vol. 14, No. 2014, pp. 23-26).

Das, S., Wang, B., & Camp, L. J. (2019, July). MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content. In *Proceedings of the Thriteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*.

Grassi, P. A.; Fenton, J.L.; Newton, E.M.; Perlner, R.; Regenscheid, A.; Burr, W.E.; Richer, J.P.; Lefkovitz, N.B.; Danker, J.M.; Choong, Y.Y.; Greene, K.; and Theofanos, M.F. Digital Identity Guidelines: Authentication and Lifecycle Management. National Institute of Standards and Technology, Special Publication (NIST SP) -800-63B (updated 2024).

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with computers*, *23*(3), 256-267.

Güven, E. Y., Boyaci, A., & Aydin, M. A. (2022). A novel password policy focusing on altering user password selection habits: a statistical analysis on breached data. *Computers & Security*, *113*, 102560.

Kagnici, O., Bisgin, H., & Uludag, S. (2025, February). Evaluating the Efficacy of GPT-based Password Generation on Real World Data. In *2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC)* (pp. 1-5). IEEE.

Marquardson, J. (2012). Password Policy Effects on Entropy and Recall: research in Progress. In: 8th Americas Conference on Information Systems. Seattle, Washington.

Merdenyan, B., Petrie, H., 2022. Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours. Behaviour & Information Technology 41 (12), 2514–2527.

Shay, R., Komanduri, S., Durity, A. L., Huh, P., Mazurek, M. L., Segreti, S. M., ... & Cranor, L. F. (2016). Designing password policies for strength and usability. *ACM Transactions on Information and System Security (TISSEC)*, *18*(4), 1-34.

Rodriguez, J.J., Zibran, M.F., Eishita, F.Z., 2022. Finding the Middle Ground: Measuring Passwords for Security and Memorability. In: Proceedings of 2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications. SERA, pp. 77–82.

Siddique, K., Akhtar, Z., & Kim, Y. (2017). Biometrics vs passwords: a modern version of the tortoise and the hare. *Computer Fraud & Security*, *2017*(1), 13-17.

Wang, P., Boodraj, M., & Baskerville, R. (2025). Beyond passwords: A review of the hidden risks in two-factor authentication. *Journal of Systems and Information Technology*, 28 (2): 173–202.

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*, *111*, 36-48.

Woods, N., Siponen, M., 2019. Improving password memorability, while not inconveniencing the user. International Journal of Human-Computer Studies 128, 61–71.

Woods, N., & Siponen, M. (2025). Questioning a security assumption: are unique passwords harder to remember than reused or modified passwords? *Computers & Security*, *157*, 104545.

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, *133*, 26-44.