The Future of Authentication: Not as Simple as Providing a Secure Solution

Naomi Woods and Hanna Paananen
University of Jyväskylä, Finland

naomi.woods@jyu.fi
hanna.k.paananen@jyu.fi

Abstract: In recent years, the number of online and digital accounts have grown, with the average user needing over 100 passwords. With so many passwords, users often struggle, and therefore, there are many password authentication alternatives on the market, including password managers, biometrics, passkeys, and multifactor authentication (MFA) to add security to passwords. All of these solutions have their pros and cons, and if the user manages them well, they are a secure means to authenticate without relying on multiple passwords and the issues that passwords bring to authentication. For several years, the technology and cybersecurity industries have been calling for the death of passwords, and yet they are still among us. Previous research has identified reasons why password alternatives and solutions are not widely accepted by users. These include users' trust, new technology usage and acceptance, perceptions of privacy, financial cost, and misguided security perceptions. With the introduction of newer and more convenient technologies such as passkeys, it is hoped that passwords will finally die. However, from initial interviews, those working in the technology and cybersecurity industries are reporting resistance from users. This study aims to examine users' perceptions of authentication methods, and their intentions for improving the security of their digital lives in the future. A mixed-method approach will conduct questionnaires, measuring user perceptions and attitudes towards authentication methods, their motivations for securing their own and organizational digital services, as well as demographic data that could indicate any interaction effect. Furthermore, interviews will be conducted to delve deeper into participants' responses. The results will shed light on factors that are influencing the uptake of secure authentication solutions, and will have several implications establishing a comprehensive view of different user factors that influence authentication decision-making that could ultimately shape the future of the authentication solution industry.

Keywords: Authentication, User behaviour, Cyber security, Security motivations

1. Introduction

Passwords remain the most common way people secure multiple accounts, but managing numerous credentials is a persistent challenge. As a result, alternatives such as password managers, biometrics, passkeys, and multifactor authentication have emerged to strengthen or replace traditional passwords. Each option brings advantages and trade-offs, yet passwords persist. Previous research points to several barriers to broader adoption of these alternatives, including trust issues, reluctance to adopt new technologies, privacy concerns, cost, and misconceptions about security (Matzen et al. 2025; Siddique et al. 2017; Wang et al. 2025; Woods & Siponen 2025). Although newer, more convenient solutions like passkeys promise to phase out passwords, user resistance continues to slow that transition (Daffalla et al. 2025; Matzen et al. 2025). Ten years ago, the promise of biometrics taking over and replacing passwords did not come to fruition, this begs the question of whether newer alternatives will really end the use of passwords? And what would it take from the users' perspective?

The objective of this study is to draw upon psychology and decision science to understand the user's influence on future authentication. It will examine users' perceptions of authentication methods, and their intentions for improving the security of their digital lives in the future. With the aim of highlighting the challenges the cybersecurity industry face when providing users with a secure means to authenticate, we aim to answer these research questions: What are the key issues that lead to users' use or reluctance to use different authentication methods? Are there common factors across all authentication methods? What will make authentication solutions usable for users in the future?

2. Overview: Current Authentication Solutions

Passwords are the most common mechanism. Their strengths include cost-effectiveness, easily deployed across multiple systems, and strong if created well. Password weaknesses arise due to multiple accounts, the users' discipline, and cognitive abilities. This can lead to weak passwords, as users struggle to remember complex passwords, which can result in password reuse (Woods & Siponen 2025). Previous research has examined the security, user behaviours, and usability issues with the aim of improving their security (Woods & Siponen 2025).

Password Managers allow users to store their passwords behind one master password or key securely. The advantages include improved security and usability of multiple passwords. The disadvantages can include cross-

device usage limitations, vulnerable to phishing, and loss or theft of the physical device (Siddique et al. 2017). Password managers were thought to answer the password memorability and security problems, however, their uptake has been low (Woods & Siponen 2025). Previous research notes that many users prefer to memorize their passwords instead of using password managers (Das et al., 2014), due to distrust (perceptions off vulnerability to attacks and trust their own memory) (Woods & Siponen 2025).

Biometrics include physical and behavioural attributes (inc. users' fingerprint, iris, face recognition, keystroke, etc.). They are convenient and strong (Siddique et al. 2017). Unfortunately, there are weaknesses including vulnerability to spoofing, privacy concerns, cost, poor accuracy, and unusable by some users. Furthermore, breaches of biometric databases are concerning as credentials cannot be revoked (Wang et al. 2025).

Token-based methods include, USB, passkeys, mobile and authenticator apps, have several advantages, such as providing higher security and reduce the need to memorize information (except for a PIN). However, their disadvantages can include inconvenience, fear of loss of physical tokens, impractical if they need to be revoked and reissued, as well as limitations in cross-device usage (Siddique et al. 2017). The uptake of these devices is mixed, as users' perceptions are influenced by ease of use, compatibility, technical support, and challenges need to be addressed for wider adoption, e.g., easier setup processes (Nanda et al. 2024).

Passkeys are considered a secure, automatic authentication method based on public-key cryptography where the user authenticates using a device and the user's biometrics or a PIN (Lassak et al. 2024; Matzen et al. 2025). However, there challenges include a lack of standardized recovery mechanisms for lost or damaged devices, compatibility issues, privacy concerns, and phishing risks to backup processes and mechanisms. There are user challenges too, such as mistrust, set-up difficulties, privacy concerns, fear of devices being damaged, and denial of services (Daffalla et al. 2025; Matzen et al. 2025; Nanda et al. 2024).

Multifactor Authentication (MFA) (inc. Two-factor Authentication (2FA)) enhances the security of authentication by requiring multiple verification factors (e.g., biometrics, tokens) (Das et al. 2019). The advantages include adding a strong security layer beyond passwords and reducing the risk of unauthorized access (Wang et al. 2025). Despite its security benefits, MFA has its challenges including, complex enrolment and backup processes, inconvenient, complex, and frustrating authentication processes (Das et al. 2019; Klivan et al. 2023; Wang et al. 2025).

3. Is History Going to Repeat Itself? Motivations for Proposed Study

Previous research has noted that user perceptions are critical for accepting authentication schemes (Zimmermann & Gerber 2020), and low adoption can be due to for example, the difference between users' objectivity and subjectivity when considering new authentication methods, influencing their familiarity, trust, ease of use, and perceptions of complexity, reliability, and costs (Klivan et al. 2023; Wang et al. 2025). Furthermore, usability problems discourage adoption leading to choosing less secure options (Das, et al. 2019).

New authentication solutions like passkeys have the potential to revolutionize authentication systems, but also face significant challenges in user perceptions, technical implementation, and usability (Daffalla et al. 2025; Matzen et al. 2025). Preliminary interviews of experts working in the cybersecurity industry have reported resistance from users in using MFA and passkeys. As seen with password managers, users feel that removing their input out of the authentication process justifies distrust and feeling of a lack of control over their security. This suggests that hoping these solutions will replace passwords may be short lived. Therefore, we need to understand and identify what it would take for users to accept a secure solution to authenticate, this can bring to light key factors underlying the future uptake of authentication solutions.

4. Proposed Research Methods: Mixed Method Study

A mixed-method approach will conduct questionnaires measuring users' perceptions and attitudes towards authentication methods using items from the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al. 2017). Further items evaluating protection motivation (PMT) towards participants' own digital security and the security of their organizations will measure perceived vulnerability, severity, self-efficacy, response efficacy, and response costs (Moody & Siponen 2018). Semi-structured interviews will be conducted using established guidelines (Myers 2013). We will delve deeper into participants' questionnaire responses and discuss their perceptions towards using different authentication methods. The interview data will be transcribed and coded by two coders who are guided by verified data analysis methods (Myers 2013). The participants will be recruited from various organizations within different industries where employees are required to

authenticate using different methods. Due to this mixed-methods study taking a more qualitative approach, we will aim to recruit 15-25 participants (or more until saturation has been reached) (Myers 2013).

Ethical considerations will be taken into account, and ethical clearance from the institution's ethical committee will be sought. Participants' consent will be obtained, information including privacy policies will be provided to the participants, and data collected will be kept confidential and coded.

5. Conclusion

Over twenty years ago, Bill Gates said that passwords were dead and that biometrics would take over. The misconception that biometrics would completely replace passwords as the ultimate authentication method has set digital security especially password security, back considerably, in terms of suppressing password research and industry developments (Herley & van Oorschot 2011; Siddique et al. 2017). Even with all the digital advances, this prediction has not come true, and password authentication remains very much unchanged. In more recent times, there have been developments in authentication, bringing new secure methods to the market, with a lot of promise to finally end passwords. However, many users continue to prefer passwords and are reluctant in using other authentication methods. Getting rid of passwords is enticing, but practically it opens up several issues and difficulties. To replace passwords several concerns need to be addressed. This study proposes a mixed-method approach to fully understand these issues, specifically from the perspective of the user. The results will shed light on factors that are influencing the uptake of secure authentication solutions, and will have several implications establishing a comprehensive view of different user factors that influence authentication decision-making that could ultimately shape the future of the authentication solution industry.

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

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

References

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)*.

Herley, C., & Van Oorschot, P. (2011). A research agenda acknowledging the persistence of passwords. *IEEE Security & privacy*, *10*(1), 28-36.

Klivan, S., Höltervennhoff, S., Huaman, N., et al. (2023, November). " We've Disabled MFA for You": An Evaluation of the Security and Usability of MFA Recovery Deployments. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 3138-3152).

Lassak, L., Pan, E., Ur, B., & Golla, M. (2024). Why aren't we using passkeys? Obstacles companies face deploying {FIDO2} passwordless authentication. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 7231-7248).

Matzen, A., Rüffer, A., Byllemos, M., Heine, O., Papaioannou, M., Choudhary, G., & Dragoni, N. (2025). Challenges and potential improvements for passkey adoption—a literature review with a user-centric perspective. *Applied Sciences*, *15*(8), 4414.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance1. *MIS quarterly*, *42*(1), 285-311.

Myers, M. D. (2013). *Qualitative research in business and management*, London: Sage Publications.

Nanda, A., Jeong, J. J., Shah, S. W. A., Nosouhi, M., & Doss, R. (2024). Examining usable security features and user perceptions of Physical Authentication Devices. *Computers & Security*, *139*, 103664.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40-51.

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*.

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.