Mapping the Authentication Landscape: A User-Centric View

Hanna Paananen[1], Naomi Woods[1] and Steven Furnell[2]
[1]Faculty of Information Technology, University of Jyväskylä, Finland
[2]School of Computer Science, Faculty of Science, University of Nottingham, UK

hanna.k.paananen@jyu.fi
naomi.woods@jyu.fi
steven.furnell@nottingham.ac.uk

Abstract: Authentication is the frontline security control that protects the digitalised society—and paradoxically, it is also the most frequently exploited in breaches. As online services permeate every aspect of life, from banking and healthcare to workplace systems, authentication has become a critical safeguard for citizens and organisations. Yet, the complexity of managing multiple credentials and diverse authentication methods introduces vulnerabilities that attackers routinely exploit. Despite this, research has often examined authentication in isolation—focusing on single methods or user behaviours—without considering the broader ecosystem users navigate daily. This paper reframes authentication as an authentication landscape, a multidimensional environment encompassing all features and experiences users encounter when accessing digital systems. Through a systematic literature review of 43 peer-reviewed articles from leading Information Systems, Cybersecurity, and Human-Computer Interaction journals, we identify ten key features shaping this landscape: (1) services and systems, (2) diversity of methods, (3) guidance and restrictions, (4) devices, (5) security products, (6) use context, (7) culture and relationships, (8) user responsibilities, (9) accessibility, and (10) threat outlook. Our analysis reveals that authentication complexity—driven by proliferating accounts, evolving technologies, and inconsistent policies—creates fertile ground for security lapses. Different aspects of the landscape may lead users to trade security for convenience, adopt risky coping strategies, or struggle with contradictory guidance, amplifying systemic vulnerabilities. The implications are urgent: strengthening authentication cannot rely on piecemeal improvements to individual methods when advances in technology demand a comprehensive readjustment. Designers, policymakers, and security professionals must address the authentication landscape holistically to reduce attack surfaces and enhance resilience. Future research can operationalise the identified features to study users' landscape perception. For practice, this perspective informs the design of authentication systems and awareness programs that align with users' lived realities. By recognising authentication as a complex, interconnected landscape, we advance the discourse toward strategies that safeguard not just individual accounts but the integrity of the digital society itself.

Keywords: Authentication, User, Literature review

1. Introduction

Authenticating with online services and devices is a task most people do daily in a digitalised society. As employees they use multiple systems for work and their personal lives are managed through online systems for banking, shopping, and even identification documents (Cheswick, 2013; Kruzikova *et al.*, 2022). Both the productivity at workplaces as well as people's welfare are now dependent on authentication that permits access to these systems and restricts unwanted tampering.

Passwords are widely provided as an authentication mechanism because they are easy for users to adopt and for system developers to implement (Bonneau *et al.*, 2015; Furnell, 2022). Each user may have dozens of password-authenticated accounts across their private and work systems (Dhamija and Dusseault, 2008; Helkala and Bakås, 2014). However, the authentication market is changing rapidly through new innovations, standards, and legislation. We have come to a situation where the increasing number of digital services provides people with more options, and they may choose another service if they dislike some features, such as the authentication method (Kruzikova *et al.*, 2022; Taherdoost, 2017). On the other hand, corporate policies may contribute to the increased amount of credentials when they require work and personal accounts to be separate (Dhamija and Dusseault, 2008). All this leads to users spending a considerable amount of their time logging into different systems (Bhana and Flowerday, 2020).

Research literature largely focuses on user interactions with authentication methods but does not consider how this might be affected when the user operates in the landscape of authentication. The landscape metaphor is used here to draw attention to the fact that each user views a plethora of authentication-related features from their own vantage point while another user may view the same things from another perspective. Literature has primarily focused on improving the design of authentication methods or the security behaviour of the users. Here we shift the focus from the single user, single authentication mechanism and zoom out to the entire authentication landscape with the aim of conceptualizing this level of analysis. There are very few studies that have explored users' perceptions of authentication as a daily activity spanning all walks of life. One exception is

a diary study that was carried out to see how people cope with passwords in their daily lives (Grawemeyer and Johnson, 2011).

There are several forces influencing the authentication landscape that have been discussed in research literature. Our aim is to understand *what kind of features users perceive in the authentication landscape*. We will answer this question by reviewing research literature on user aspects of authentication. We will first present our review method and then present the authentication features we recognized. Lastly, we discuss the implications and offer conclusions.

2. Survey Method

The literature for this review was selected using a modified systematic review method (Okoli, 2015). The search was limited to 25 prominent journals in fields of information systems, cybersecurity and human-computer interaction to avoid including substandard, non-peer reviewed papers. We used Elsevier Scopus as the search database. The search term included selected journals and a word search of *authentication OR password* AND user* in article title, abstract and keywords. The search resulted in a list of 647 articles which were first evaluated by title and then by abstract. This resulted in a list of 155 articles for full text evaluation and 43 were included for having themes relating to authentication landscape. We excluded papers not related to the research question, published before 2000, and without user point-of-view. The sample was analysed using interpretive thematic clustering.

3. User Authentication

Authentication methods are often divided into three categories: knowledge-based, token, and biometric (Bhana and Flowerday, 2020). Passwords are the most used authentication method (Furnell, 2022) and the best-known knowledge-based method. PIN numbers or longer passphrases may use a similar interface but different rules for forming the secret (Bhana and Flowerday, 2022). Another category of knowledge-based authentication methods is the graphical password, and probably the best-known type is the Android pattern-lock that uses a three-by-three grid where a pattern is drawn (Cho *et al.*, 2020). Biometrics have also gained popularity over the years as sensor technologies have been added to personal devices, such as smartphones. The fingerprint is the most popular biometric, even when face recognition or iris scan would be an option (Cho *et al.*, 2020). Smartphones are often also used in token-based authentication as a trusted device (Constantinides *et al.*, 2023). These authentication methods can be used as combinations in multi-factor authentication to increase security if one factor is compromised and tokens are commonly used as the additional factor (Weir *et al.*, 2010).

Authentication methods cannot be examined in isolation as each user may have several user accounts in both their personal and professional lives. This creates a problem for knowledge-based passwords, which people tend to reuse to reduce the number of secrets but, at the same time, create opportunities for malicious actors to enter several systems with one leaked password (Campbell *et al.*, 2011; Woods and Siponen, 2024). Similarly, dedicated tokens may create the issue of needing to match the token with the correct account (Weir *et al.*, 2010). There are solutions that users can use to mitigate the problems created by multiple credentials, such as password managers (Bonneau *et al.*, 2015). Federated authentication allows login with third-party credentials such as the “Login with Facebook” provided in many consumer services. Some users may avoid this option due to privacy concerns. (Bonneau *et al.*, 2015; Satchell *et al.*, 2011.)

3.1 Authentication Landscape

When we consider the authentication landscape, we focus on a combination of features that the user perceives when interacting with the digital world. This point-of-view differs from studies that focus on qualities of individuals such as self-efficacy (Dodel and Mesch, 2019; Mattson *et al.*, 2023), anxiety (Woods and Siponen, 2024) or IT security diligence (Datta and Krancher, 2024). It also extends the view from studying single types of authentication instances such as passwords or devices. In the following sections we discuss the authentication landscape features we identified in the 42 articles in our literature sample by interpretive thematic clustering.

3.1.1 Services and systems

The security of the digital world can appear very differently to people depending on what type and how many systems or online services they use. People in IT related jobs have even reported having “hundreds” of accounts which can lead to using less secure coping strategies (Wolf et al., 2018). People may use stronger authentication methods or unique passwords for systems with sensitive information (Crossler and Posey, 2017; Grawemeyer and Johnson, 2011). For example, stronger passwords are used for online banking due to the clear personal loss

that could result from a security breach while convenience is valued more in services like email, where the repercussions are less obvious (Tam et al., 2010).

3.1.2 Diversity of methods

The diversity of systems comes with the diversity of authentication methods. The password may be seen as being problematic if there are too many and they change too often (Hadzidedic *et al.*, 2022). There may be alternatives to passwords depending on the service or device. Performance of the methods such as perceived time spent and success rate influence users' preferences (Ibrahim *et al.*, 2019; Kruzikova *et al.*, 2024). Familiarity with methods such as biometrics affects how users perceive their security and convenience (Breward *et al.*, 2017). A single site can offer several alternative authentication methods such as SSO logins, but their usefulness depends on the service provider and if other sites provide the same option (Morkonda *et al.*, 2024). Furthermore, when MFA is used it may use a combination of various types of authenticators, such as security apps or dedicated devices (Sinigaglia et al. 2020).

3.1.3 Guidance and restrictions

The correct use of authentication methods affects their security, which is why users are subjected to different types of guidance and restrictions when authenticating. Users may be gently nudged in the right direction to make better decisions while creating passwords (Kaleta *et al.*, 2019). In organisations the password creation policies may be more compelling and require more secure passwords (Florêncio *et al.*, 2016). Password composition policies may also be technically implemented (Bargas-Avila *et al.*, 2011). However, users may find it confusing when different online services have different requirements for password composition (Cheswick, 2013; Furnell, 2024).

3.1.4 Devices

The devices that people use also play a role in how people perceive authentication. The different hardware and software features across devices affect what types of authentication options are available (Botha *et al.*, 2009). Then again, a single device like the smartphone can offer several different authentication options that can be activated and used interchangeably (Cho *et al.*, 2020). The use experience of authentication methods may vary across devices since their input systems are different (Forget *et al.*, 2015). The novelty of the device and user's skills in using it also affect the authentication experience (Kruzikova *et al.*, 2022).

3.1.5 Security products

Security-related services may affect the authentication mechanisms and how they are used. These include password managers, SSO/identity management, physical authentication devices, and security software which may be free to use or paid services. It has been found that less than half of people are willing to pay for federated identity management, even though the free versions (e.g., login with Facebook or Google) have been deemed questionable in protecting the users' privacy (Roßnagel *et al.*, 2014). Also, the cost of switching to such systems may not only be monetary but require substantial effort (Renaud *et al.*, 2019).

The features of security tools affect the perception people have of them such as authentication devices' physical attributes and functionalities (Nanda *et al.*, 2024). In software it can be the quality of tips provided to make security decisions (Furnell and Clarke, 2012; Ortlieb, 2014). Unfortunately, the positive experience that these services provide can also be detrimental if people engage in risky behaviour due to over-reliance on the technology's ability to protect (the Pelzman Effect) (Datta and Krancher, 2024). Then again people may also not believe that service providers are able to limit unauthorized access to their data (Crossler and Posey, 2017; Hadzidedic *et al.*, 2022).

3.1.6 Use context

Authentication is needed while acting in different roles and places. People's preferences vary depending on their surroundings such as home, office or public area (Crossler and Posey, 2017). The work environment differs from private use in many ways. At work there may be other clearer demands like production deadlines that distract people from the more ambiguous authentication security demands (Grawemeyer and Johnson, 2011). The type of work, or the workplace, can also affect authentication. Entrepreneurs tend to choose stronger passwords as they have the responsibility of the business on their shoulders (Helkala and Bakås, 2014). Then again people in state government organisations have been found to adhere better to password policies due to more training, guidance and enforcement (Fitri *et al.*, 2025).

3.1.7 Culture and relationships

The authentication landscape is also affected by users' culture and social relationships. The use of textual passwords is affected by the user's language and culture. A study on a leaked user database revealed that the most common passwords have different patterns of character use across different nationalities. (AlSabah et al., 2018.) Differences have also been found between countries on how much users tend to follow rules on password security which may be attributed to differing uncertainty avoidance across cultures (Hadzidedic et al., 2022).

Social relationships also have effects on their perception of authentication. People may worry about their shoulder surfing family members and roommates, affecting the selection of authentication methods (Ortlieb, 2014). On the other hand, social influence has a significant positive effect on trust of password managers which affects their adoption (Tian, 2024).

3.1.8 User responsibilities

Users have varying perceptions of how much their own choices influence the authentication landscape. People adapt their security behaviour according to their personal risk assessment of the digital environment (Wolf *et al.*, 2018). They may weigh risks and benefits when choosing their password management techniques (Merdenyan and Petrie, 2022). On the other hand, many have lacking and erroneous knowledge of the secure use of systems (Grawemeyer and Johnson, 2011). People need to learn the functionalities of security technologies to correctly operate them on personal devices (Furnell and Clarke, 2012). Furthermore, one time learning is not enough since technology changes over time and managing the increasing amount of credentials requires creating and adapting routines (Renaud *et al.*, 2019).

3.1.9 Accessibility

People's perceptions of the authentication landscape are also affected by their ability to operate technology. Digital divide between users means that there are notable disparities in access to digital world, such as internet use timespan and frequency, and digital safety skills (Dodel and Mesch, 2019). People may also have cognitive, sensory and physical restrictions in using authentication methods (Furnell *et al.*, 2022). Authentication often requires error-free entry and perfect recall, good memory, hearing, attention, dexterity, vision or learning (Renaud and Ramsay, 2007). New authentication innovations may need to consider user physical characteristics such as the effect of body composition on smart watch vibration detection (Lee *et al.*, 2023). Physical characteristics may also change over time which poses a challenge for biometric authentication such as facial recognition (Ibrahim *et al.*, 2019).

3.1.10 Threat outlook

A core feature of the authentication landscape is the threat outlook meaning the users' perception of threats toward the information, systems and devices that should be protected from unauthorised access. When choosing an authentication method, people weigh the perceived probability of attacks toward different methods (Kruzikova *et al.*, 2022). As technology advances new threats can emerge that could compromise for example the biometric data that is used for authentication, making it useless for future authentication (Zhang *et al.*, 2024). Centralised systems such as password managers may cause widespread problems if users' all accounts are compromised in one leak (Nehme *et al.*, 2024).

Fear against threats and the perceived ability to face them may affect authentication method use (Mattson *et al.*, 2023). Differences have been detected between regular IT users and security experts in perception of risk and using password workarounds (Rooney *et al.*, 2024). People may not comprehend how authentication protects them and understanding varies on the consequences of being victimised (Dodel and Mesch, 2019). Fear appeals may evoke the willingness to take better protective measures, but their effect deteriorates over time (Mwagwabi *et al.*, 2018).

4. Discussion

The aim of this review was to understand what kind of features users perceive in the authentication landscape. The research literature on user authentication discusses multiple features which we grouped into ten categories. Authentication is often studied from the point-of-view of a single user and a single authentication method which was prevalent in this review. We find this approach does not account for the interplay between the user's other experiences with authentication.

Many of the identified key issues span across several feature categories. These underlying themes include increasing complexity, changes over time, learning, and quality of information (and misinformation). Complexity can be detected in the increasing number of systems and authentication methods users need to adopt. When a user is presented with another authentication task, it may not matter how simple it is if it adds to the complexity of the landscape. Complexity is also one of the things that changes over time. When people create more accounts for more services over time, they increase their authentication load by creating passwords or connecting new accounts to password managers or SSO services. The authentication load gets worse as we get older and at the same time our ability to create new safer habits gets worse (Renaud and Ramsay, 2007). Our capabilities and opportunities to learn about new threats and innovations vary depending on where we work (Fitri *et al.*, 2025) and how we age. Furthermore, our perceptions of the authentication landscape are affected by the quality of the information we get from online services, security tools, social connections and employers. Acknowledging the interplay of the landscape features is important for reducing attack surfaces and increasing resilience for authentication.

Future research can utilise the identified features of authentication landscape in both qualitative and quantitative studies. A qualitative study could add understanding of the underlying themes that are still quite sparsely discussed in research literature. A quantitative study could turn the ten features into a measuring instrument that could be used for clustering users into groups that perceive the landscape in a similar way. This approach could be useful in conjunction with the choices people make, such as choosing usability over security or one method over another. When combined with observed ratings of usability and security of methods (Zimmermann *et al.*, 2019), the perceived features of authentication landscape may shed light on how the overlapping effects of features can affect decisions compared to objective ratings.

This review also comes with some limitations. Due to the overwhelming number of authentication papers and the wide scope of our research question, we could not include more than 25 journals. The analysis method used here was very free form, but future research could also attempt a more robust meta-analysis. This may be challenging as the literature on user authentication is very heterogeneous and includes a limited number of comparable variables.

5. Conclusion

This review advances the understanding of the user perspective of the authentication landscape in a digitalised society. We analysed 43 research articles on user authentication and categorised the identified issues into ten categories: services and systems, diversity of methods, guidance and restrictions, devices, security products, use context, culture and relationships, user responsibilities, accessibility, and threat outlook. These features offer a more organised look into the user perception of authentication for researchers, policymakers, designers and security professionals. They lay the groundwork for studies that aim to understand user authentication choices in relation to users' overall authentication experiences. Furthermore, system developers may consider these features when designing the authentication experience of their service.

Acknowledgements

This research was funded by Business Finland (1610/31/2022).

Ethics Declaration: Ethics clearance was not needed.

AI Declaration: DeepL was used for grammar checks.

References

AlSabah, M., Oligeri, G. and Riley, R. (2018), "Your culture is in your password: An analysis of a demographically-diverse password dataset", Computers and Security, Vol. 77, pp. 427–441, doi: 10.1016/j.cose.2018.03.014.

Bargas-Avila, J.A., Orsini, S., Piosczyk, H., Urwyler, D. and Opwis, K. (2011), "Enhancing online forms: Use format specifications for fields with format restrictions to help respondents", Interacting with Computers, Vol. 23 No. 1, pp. 33–39, doi: 10.1016/j.intcom.2010.08.001.

Bhana, B. and Flowerday, S. (2020), "Passphrase and keystroke dynamics authentication: Usable security", Computers and Security, Vol. 96, doi: 10.1016/j.cose.2020.101925.

Bhana, B. and Flowerday, S.V. (2022), "Usability of the login authentication process: passphrases and passwords", Information and Computer Security, Vol. 30 No. 2, pp. 280–305, doi: 10.1108/ICS-07-2021-0093.

Bonneau, J., Herley, C., Van Oorschot, P.C. and Stajano, F. (2015), "Passwords and the evolution of imperfect authentication", Communications of the ACM, Vol. 58 No. 7, pp. 78–87, doi: 10.1145/2699390.

Botha, R.A., Furnell, S. and Clarke, N. (2009), "From desktop to mobile: Examining the security experience", Computers and Security, Vol. 28 No. 3–4, pp. 130–137, doi: 10.1016/j.cose.2008.11.001.

Breward, M., Hassanein, K. and Head, M. (2017), "Understanding consumers' attitudes toward controversial information technologies: A contextualization approach", Information Systems Research, Vol. 28 No. 4, pp. 760–774, doi: 10.1287/isre.2017.0706.

Campbell, J., Ma, W. and Kleeman, D. (2011), "Impact of restrictive composition policy on user password choices", Behaviour and Information Technology, Vol. 30 No. 3, pp. 379–388, doi: 10.1080/0144929X.2010.492876.

Cheswick, W. (2013), "Rethinking passwords", Communications of the ACM, Vol. 56 No. 2, pp. 40–44, doi: 10.1145/2408776.2408790.

Cho, G., Huh, J.H., Kim, S., Cho, J., Park, H., Lee, Y., Beznosov, K., et al. (2020), "On the Security and Usability Implications of Providing Multiple Authentication Choices on Smartphones: The More, the Better?", ACM Transactions on Privacy and Security, Vol. 23 No. 4, doi: 10.1145/3410155.

Constantinides, A., Belk, M., Fidas, C., Beumers, R., Vidal, D., Huang, W., Bowles, J., et al. (2023), "Security and Usability of a Personalized User Authentication Paradigm: Insights from a Longitudinal Study with Three Healthcare Organizations", ACM Transactions on Computing for Healthcare, ACM PUB27 New York, NY , Vol. 4 No. 1, doi: 10.1145/3564610.

Crossler, R.E. and Posey, C. (2017), "Robbing peter to pay paul: Surrendering privacy for security's sake in an identity ecosystem", Journal of the Association for Information Systems, Vol. 18 No. 7, pp. 487–515, doi: 10.17705/1jais.00463.

Datta, P.M. and Krancher, O. (2024), "Cybersecurity end-user compliance: Password management versus update compliance", Information & Management, North-Holland, Vol. 61 No. 8, pp. 1–16, doi: 10.1016/J.IM.2024.104060.

Dhamija, R. and Dusseault, L. (2008), "The seven flaws of identity management: Usability and security challenges", IEEE Security and Privacy, Vol. 6 No. 2, pp. 24–29, doi: 10.1109/MSP.2008.49.

Dodel, M. and Mesch, G. (2019), "An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices", Computers and Security, Vol. 86, pp. 75–91, doi: 10.1016/j.cose.2019.05.023.

Fitri, R.D., Hilman, M. and Yazid, S. (2025), "Improving password policy strategies: a government employee perspective", Information and Computer Security, Emerald Publishing, Vol. ahead-of-print No. ahead-of-print, doi: 10.1108/ICS-12-2024-0335/FULL/PDF.

Florêncio, D., Herley, C. and Van Oorschot, P.C. (2016), "Pushing on string: The 'Don't care' region of password strength", Communications of the ACM, Vol. 59 No. 11, pp. 66–74, doi: 10.1145/2934663.

Forget, A., Chiasson, S. and Biddle, R. (2015), "User-centred authentication feature framework", Information and Computer Security, Vol. 23 No. 5, pp. 497–515, doi: 10.1108/ICS-08-2014-0058.

Furnell, S. (2022), "Assessing website password practices – Unchanged after fifteen years?", Computers and Security, Elsevier Ltd, Vol. 120, doi: 10.1016/J.COSE.2022.102790.

Furnell, S. (2024), "Usable Cybersecurity: a Contradiction in Terms?", Interacting with Computers, Oxford Academic, Vol. 36 No. 1, pp. 3–15, doi: 10.1093/IWC/IWAD035.

Furnell, S. and Clarke, N. (2012), "Power to the people? the evolving recognition of human aspects of security", Computers and Security, Vol. 31 No. 8, pp. 983–988, doi: 10.1016/j.cose.2012.08.004.

Furnell, S., Helkala, K. and Woods, N. (2022), "Accessible authentication: Assessing the applicability for users with disabilities", Computers and Security, Vol. 113, doi: 10.1016/j.cose.2021.102561.

Grawemeyer, B. and Johnson, H. (2011), "Using and managing multiple passwords: A week to a view", Interacting with Computers, Vol. 23 No. 3, pp. 256–267, doi: 10.1016/j.intcom.2011.03.007.

Hadzidedic, S., Fajardo-Flores, S. and Ramic-Brkic, B. (2022), "User perceptions and use of authentication methods: insights from youth in Mexico and Bosnia and Herzegovina", Information and Computer Security, Vol. 30 No. 4, pp. 615–632, doi: 10.1108/ICS-07-2021-0105.

Helkala, K. and Bakås, T.H. (2014), "Extended results of Norwegian password security survey", Information Management and Computer Security, Vol. 22 No. 4, pp. 346–357, doi: 10.1108/IMCS-10-2013-0079.

Ibrahim, T.M., Abdulhamid, S.M., Alarood, A.A., Chiroma, H., Al-garadi, M.A., Rana, N., Muhammad, A.N., et al. (2019), "Recent advances in mobile touch screen security authentication methods: A systematic literature review", Computers and Security, Vol. 85, pp. 1–24, doi: 10.1016/j.cose.2019.04.008.

Kaleta, J.P., Lee, J.S. and Yoo, S. (2019), "Nudging with construal level theory to improve online password use and intended password choice: A security-usability tradeoff perspective", Information Technology and People, Vol. 32 No. 4, pp. 993–1020, doi: 10.1108/ITP-01-2018-0001.

Kruzikova, A., Knapova, L., Smahel, D., Dedkova, L. and Matyas, V. (2022), "Usable and secure? User perception of four authentication methods for mobile banking", Computers & Security, Elsevier Advanced Technology, Vol. 115, p. 102603, doi: 10.1016/J.COSE.2022.102603.

Kruzikova, A., Muzik, M., Knapova, L., Dedkova, L., Smahel, D. and Matyas, V. (2024), "Two-factor authentication time: How time-efficiency and time-satisfaction are associated with perceived security and satisfaction", Computers and Security, Elsevier Ltd, Vol. 138, doi: 10.1016/j.cose.2023.103667.

Lee, S., Choi, W. and Lee, D.H. (2023), "The vibration knows who you are! A further analysis on usable authentication for smartwatch users", Computers and Security, Vol. 125, doi: 10.1016/j.cose.2022.103040.

Mattson, T., Aurigemma, S. and Ren, J. (2023), "Positively Fearful: Activating the Individual's HERO Within to Explain Volitional Security Technology Adoption", Journal of the Association for Information Systems, Vol. 24 No. 3, pp. 664–699, doi: 10.17705/1jais.00793.

Merdenyan, B. and Petrie, H. (2022), "Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours", Behaviour and Information Technology, Vol. 41 No. 12, pp. 2514–2527, doi: 10.1080/0144929X.2021.2019832.

Morkonda, S.G., Chiasson, S. and van Oorschot, P.C. (2024), "Influences of displaying permission-related information on web single sign-on login decisions", Computers and Security, Elsevier Ltd, Vol. 139, doi: 10.1016/j.cose.2023.103666.

Mwagwabi, F., McGill, T. and Dixon, M. (2018), "Short-term and long-term effects of fear appeals in improving compliance with password guidelines", Communications of the Association for Information Systems, Vol. 42 No. 1, pp. 147–182, doi: 10.17705/1CAIS.04207.

Nanda, A., Jeong, J.J., Shah, S.W.A., Nosouhi, M. and Doss, R. (2024), "Examining usable security features and user perceptions of Physical Authentication Devices", Computers and Security, Elsevier Ltd, Vol. 139, doi: 10.1016/j.cose.2023.103664.

Nehme, A., Li, M. (Leah) and Warkentin, M. (2024), "Adaptive and maladaptive factors behind password manager use: A hope-extended protection motivation perspective", Computers & Security, Elsevier Advanced Technology, Vol. 144, p. 103941, doi: 10.1016/J.COSE.2024.103941.

Okoli, C. (2015), "A Guide to Conducting a Standalone Systematic Literature Review", Communications of the Association for Information Systems.

Ortlieb, M. (2014), "The anthropologist's view on privacy", IEEE Security and Privacy, Vol. 12 No. 3, pp. 85–87, doi: 10.1109/MSP.2014.57.

Renaud, K., Otondo, R. and Warkentin, M. (2019), "'This is the way "I" create my passwords'.. does the endowment effect deter people from changing the way they create their passwords?", Computers and Security, Vol. 82, pp. 241–260, doi: 10.1016/j.cose.2018.12.018.

Renaud, K. and Ramsay, J. (2007), "Now what was that password again? A more flexible way of identifying and authenticating our seniors", Behaviour and Information Technology, Vol. 26 No. 4, pp. 309–322, doi: 10.1080/01449290601173770.

Rooney, M.J., Levy, Y., Li, W. and Kumar, A. (2024), "Comparing experts' and users' perspectives on the use of password workarounds and the risk of data breaches", Information and Computer Security, Emerald Publishing, Vol. 33 No. 2, pp. 196–222, doi: 10.1108/ICS-05-2024-0116/FULL/PDF.

Roßnagel, H., Zibuschka, J., Hinz, O. and Muntermann, J. (2014), "Users' willingness to pay for web identity management systems", European Journal of Information Systems, Vol. 23 No. 1, pp. 36–50, doi: 10.1057/ejis.2013.33.

Satchell, C., Shanks, G., Howard, S. and Murphy, J. (2011), "Identity crisis: User perspectives on multiplicity and control in federated identity management", Behaviour and Information Technology, Vol. 30 No. 1, pp. 51–62, doi: 10.1080/01449290801987292.

Taherdoost, H. (2017), "Understanding of e-service security dimensions and its effect on quality and intention to use", Information and Computer Security, Vol. 25 No. 5, pp. 535–559, doi: 10.1108/ICS-09-2016-0074.

Tam, L., Glassman, M. and Vandenwauver, M. (2010), "The psychology of password management: A tradeoff between security and convenience", Behaviour and Information Technology, Vol. 29 No. 3, pp. 233–244, doi: 10.1080/01449290903121386.

Tian, X. (2024), "Unraveling the dynamics of password manager adoption: a deeper dive into critical factors", Information and Computer Security, Emerald Publishing, Vol. 33 No. 1, pp. 117–139, doi: 10.1108/ICS-09-2023-0156/FULL/PDF.

Weir, C.S., Douglas, G., Richardson, T. and Jack, M. (2010), "Usable security: User preferences for authentication methods in eBanking and the effects of experience", Interacting with Computers, Vol. 22 No. 3, pp. 153–164, doi: 10.1016/j.intcom.2009.10.001.

Wolf, F., Kuber, R. and Aviv, A.J. (2018), "An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication", Behaviour and Information Technology, Vol. 37 No. 4, pp. 320–334, doi: 10.1080/0144929X.2018.1436591.

Woods, N. and Siponen, M. (2024), "How memory anxiety can influence password security behavior", Computers & Security, Elsevier Advanced Technology, Vol. 137, p. 103589, doi: 10.1016/J.COSE.2023.103589.

Zhang, J., Liu, Z. and Luo, X. (Robert). (2024), "Unraveling juxtaposed effects of biometric characteristics on user security behaviors: A controversial information technology perspective", Decision Support Systems, North-Holland, Vol. 183, p. 114267, doi: 10.1016/J.DSS.2024.114267.

Zimmermann, V., Gerber, N., Mayer, P., Kleboth, M., von Preuschen, A. and Schmidt, K. (2019), "Keep on rating – on the systematic rating and comparison of authentication schemes", Information and Computer Security, Vol. 26 No. 5, pp. 621–635, doi: 10.1108/ICS-01-2019-0020.