A Maturity Model for Password Security Education

Georgia Barnard and Tapiwa Gundu
Nelson Mandela University, South Africa

tapgun@gmail.com

Abstract. This paper introduces the Password Security Education Maturity Model (PSEMM), a comprehensive framework designed to guide organizations in systematically improving their password security practices through a structured progression of educational and operational stages. The model delineates five levels of maturity, Naivety, Foundational Awareness, Active Engagement, Embedded Security Habits, and Adaptive Security Mindset each representing a step forward in the development of robust password security protocols and a culture of security awareness. The development of the PSEMM is grounded in a systematic literature review (SLR) that identified 989 articles that were then screened for inclusion eligibility, which eventually resulted in 12 articles being used to identify key themes and gaps in existing cybersecurity education models. Through this rigorous analysis, the study pinpointed the need for a specialized maturity model that not only addresses the technical aspects of password management but also emphasizes the critical role of continuous education and employee engagement. The PSEMM fills this gap by offering a clear, adaptable pathway for organizations of varying sizes and sectors to enhance their cybersecurity posture. The model's applicability is demonstrated through its alignment with modern security practices, such as multi-factor authentication and password management tools, ensuring its relevance in today's rapidly evolving digital terrain. This paper contributes to the field of cybersecurity education by providing a validated, practical tool for systematically advancing password security across organizational contexts. The PSEMM stands as a vital resource for organizations seeking to mitigate the risks associated with poor password practices, ultimately fostering a more resilient cybersecurity environment.

Keywords: Password security, Education maturity model, Cybersecurity, Password management, Security awareness and cybersecurity posture

1. Introduction

Password security remains a critical yet often overlooked aspect of organisational cybersecurity (Bhana and Flowerday, 2021). Despite widespread awareness of the risks associated with weak or reused passwords, recent reports continue to show that password-related breaches account for a significant portion of cyber incidents (Aslan et al., 2023). For example, the Verizon Data Breach Investigations Report revealed that over 80% of breaches involving hacking leveraged stolen or weak passwords (Verizon 2024 DBIR, 2024.). This statistic underscores the ongoing challenge organisations face in instilling effective password practices among their employees.

Furthermore, traditional password security education programs are often inconsistent and fail to address the diverse needs of modern organisations. These programmes typically focus on basic compliance rather than fostering a deep, organisational-wide culture of security (Juozapavičius et al., 2022). As a result, there is a critical need for structured frameworks that can guide organisations through a progressive improvement of their password security education efforts (Hu et al., 2022). This gap in the existing literature and practice highlights the necessity of a maturity model that not only assesses current practices but also provides a clear pathway for advancement (Muronga et al., 2019). This paper addresses this gap by introducing a Password Security Education Maturity Model (PSEMM). The model offers a structured approach for organisations to enhance their password security practices systematically. Specifically, this paper makes the following contribution:

It introduces a novel maturity model that categorises organisational password security education into five levels: Awareness, Implementation, Enhancement, Optimisation, and Mastery.

The remainder of this paper is structured as follows: Section 2 provides a comprehensive review of the existing literature on password security education, highlighting the key challenges and gaps that necessitate the development of a new maturity model. Section 3 details the methodology used to construct the Password Security Education Maturity Model (PSEMM), including the systematic literature review and criteria selection processes. In Section 4, the PSEMM is introduced, with each level of the model explained in terms of its specific objectives, practices, and expected outcomes. Section 5 presents the results of applying the PSEMM to various organizational contexts, illustrating its practical utility and effectiveness. Section 6 discusses the implications of the model, its potential impact on organizational cybersecurity, and its limitations. Finally, Section 7 concludes the paper by summarizing the key findings, outlining future research directions, and offering recommendations for implementing the PSEMM in practice.

2. Related Literature

To develop a robust framework for improving password security education, it is essential to understand the existing body of research that addresses both password management and cybersecurity education. This section reviews the relevant literature, focusing on the various maturity models that have been proposed for cybersecurity, the specific challenges of password security in organizational settings, and the educational initiatives aimed at enhancing security awareness among employees. By critically analyzing these studies, we identify the gaps and limitations that the proposed Password Security Education Maturity Model (PSEMM) seeks to address. The literature reviewed includes established maturity models like the Capability Maturity Model (CMM) and the Information Security Maturity Model (ISMM), as well as contemporary research on password security practices and the effectiveness of security training programs.

2.1 Passwords

Passwords are essential for protecting sensitive information from cyberattacks. Passwords typically consist of a combination of characters, letters, numbers, and sometimes phrases. This allows users to gain authorised access to devices, websites, and applications.

There is a need to practice password hygiene which involves the thorough and careful process of creating, organising, and securing strong passwords to strengthen the protection of systems and accounts against potential cyber threats (Juozapavičius et al., 2022). This practice is especially critical in the context of single-factor authentication systems, as many security vulnerabilities arise from the use of weak or repetitive passwords (Juozapavičius et al., 2022). Safe password practices can be taught through various security education initiatives such as classroom training, virtual training, simulation training, etc all focusing on password hygiene.

2.2 Security Education Initiatives

Security education initiatives are systematic programmes and activities that aim to increase employees' awareness, comprehension, and use of security best practices inside an organisation (Khan et al., 2011). These programmes aim to build a security-conscious culture, lower the risk of security events, and improve the organisation's overall security posture (Bauer et al., 2013).

Security education initiatives are critical for strengthening an organisation's cyber defences through enhancing employees' comprehension and implementation of security best practices (Bashorun et al., 2013). Creating and managing passwords is one of these initiatives regular training programmes, which ensures staff members understand the value of using password managers and creating secure, one-of-a-kind passwords (Siponen et al., 2014).

2.3 Maturity Models

Password management maturity models and password security education maturity models both aim to enhance cybersecurity but differ in focus and implementation. Password management maturity models assess an organization’s ability to implement and enforce secure password policies, such as multi-factor authentication (MFA), password complexity requirements, credential management, and passwordless authentication. These models help organizations transition from weak, inconsistent password practices to automated and highly secure password management systems. In contrast, password security education maturity models evaluate how well an organization educates users on secure password practices through awareness programs, training, and behavioral change initiatives. This model progresses from basic awareness campaigns to comprehensive cybersecurity training, including phishing simulations and continuous education on emerging threats. While password management maturity focuses on technological and policy-driven improvements, password security education maturity prioritizes user awareness and behavior modification. An optimal cybersecurity strategy integrates both models to ensure robust password policies while fostering a culture of security awareness (Lasrado et al., 2015.).

Maturity models have long been used as a framework for assessing and improving organizational processes. The Capability Maturity Model (CMM), for example, has been widely adopted in software development and cybersecurity to evaluate an organization’s process maturity (Yeo and Ren, 2009). Similarly, the Information Security Maturity Model (ISMM) and the Cybersecurity Capability Maturity Model (C2M2) provide structured approaches for enhancing information security practices (Rabii et al., 2020). However, these models often treat password security as a minor component within a broader cybersecurity framework, leaving a significant gap in targeted password security education. By applying this concept to the context of password security

education, organisations can develop a model to evaluate and improve their strategies for educating personnel about password security.

Maturity models provide structured frameworks that organizations use to assess and enhance their capabilities in various domains, including password management and identity and access management (IAM). In password management, maturity models help organizations evaluate their current practices and identify areas for improvement to bolster security. For example, TDi Technologies outlines a Password Management Maturity Model with five distinct levels, each building upon the previous to add complexity and security measures, thereby reducing threats from compromised passwords (Hussey, 2021).

Similarly, IAM maturity models assist organizations in understanding and advancing their IAM practices. Zluri's guide to the Identity & Access Management Maturity Model describes four levels of IAM maturity, each signifying a specific stage of development and sophistication in IAM practices (Zluri, 2024). These models typically progress through stages such as (Bitwarden, 2025; Hein-Pensel et al., 2023; Hussey, 2024; Keeper, 2025; Zluri, 2024). These levels are usually hierarchical, with each level building upon the previous one, examples include:

1.Initial 2.Repeatable 3. Defined 4. Managed 5. Optimising

Each level represents an increase in the ability to manage processes or achieve goals with greater efficiency and effectiveness.

3. Methodology

This study employed a systematic literature review (SLR) to comprehensively examine the current state of password security education and the development of maturity models within this context. Alternative research methods, such as empirical studies or surveys, were considered but ultimately not selected. While these methods could provide in-depth insights into specific organisational contexts, they would not offer the comprehensive overview necessary for developing a generalisable maturity model. The systematic literature review approach was chosen for its ability to synthesise a wide range of studies, providing a solid foundation for the development of the Password Security Education Maturity Model (PSEMM).

A systematic literature review is a methodical approach to analysing academic literature on a specific topic (Sauer and Seuring, 2023). This approach entails precise criteria for selecting literature, a thorough search strategy, and a systematic procedure for assessing, extracting, and synthesising data. It was essential to adhere to a structured process to guarantee thoroughness, transparency, and reproducibility.

The review was guided by the following research questions: (1) What are the existing models for password security education? (2) How do organisations implement these programmes? (3) What factors influence the effectiveness of password security education?

3.1 SLR Process

A comprehensive search was done using the following electronic databases; Scopus, ScienceDirect, IEEE Xplore and Google Scholar. Keywords included “Passwords”, “Cybersecurity Training “, “Security Educations”, “Maturity Models” and “Passwords Security”. The selection of databases was driven by the need to access a broad range of high-quality, peer-reviewed studies. IEEE Xplore and Scopus were chosen for their focus on technology and cybersecurity, while ScienceDirect provided access to educational research. The keywords were carefully chosen to balance specificity with breadth, ensuring that the review captured both focused studies on password security and broader research on cybersecurity education. The inclusion criteria were designed to maintain the review's relevance and academic rigor, focusing on recent, peer-reviewed articles that directly addressed the research questions. The systematic literature review process followed for this study is summarized in figure 1.

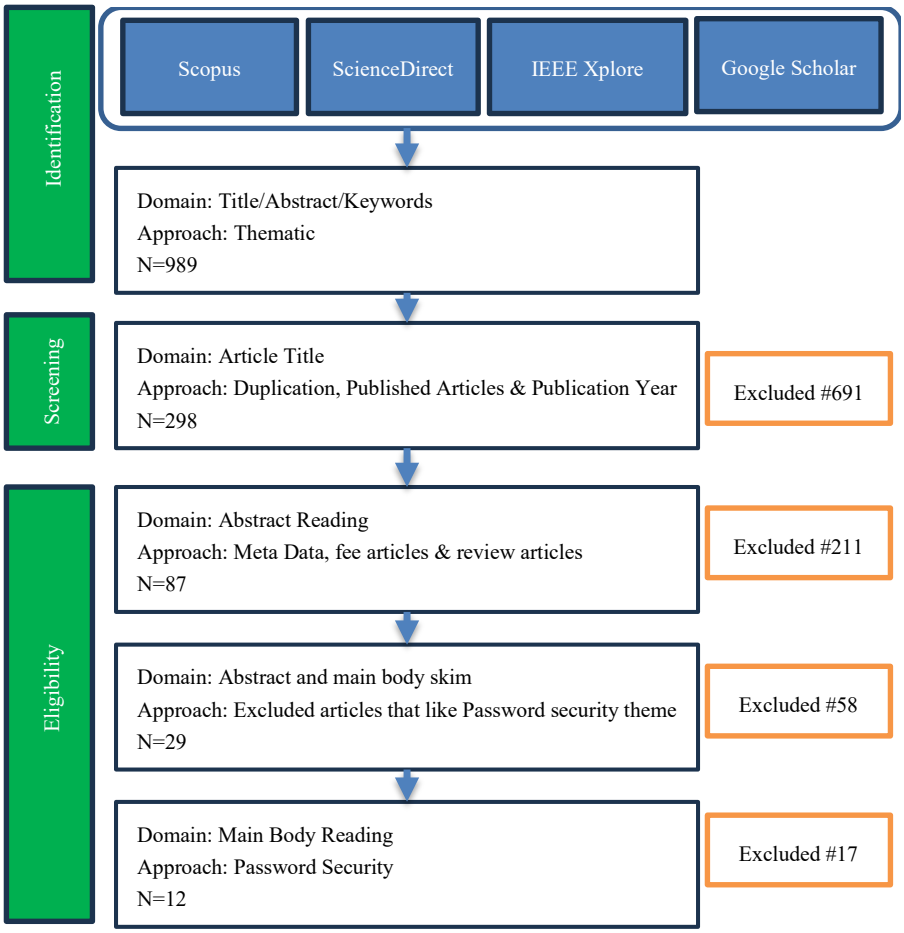

Figure 1: Systematic Literature Review Process

4. Results

The analysis of the systematic literature review revealed key themes around the progression of password security education within organisations. These themes (Table 1) emerged as foundational constructs of the proposed Password Security Education Maturity Model (PSEMM).

Table 1: Themes identified through SLR

Theme	Articles
Naivity	(Alqahtani, 2022; Gundu, 2024; Solomon et al., 2022)
Awareness	(Gundu and Modiba, 2020; Juozapavičius et al., 2022; Oesch et al., 2022)
Active Engagement	(Bhana and Flowerday, 2021; Gundu, 2023; Huang et al., 2024)
Embedded Security Habits	(Bhana and Flowerday, 2021; Chatzoglou et al., 2024; Oesch et al., 2022)
Adaptive Security Mindset	(Ezugwu et al., 2023; Farshim and Tessaro, 2021)

The identified themes include Awareness, where organisations focus on building a basic understanding of password security among employees; Implementation, where foundational security practices, such as the use of unique passwords and two-factor authentication, are put into action; Enhancement, where organisations begin to adopt more advanced practices like the use of passphrases and multi-factor authentication; Optimisation, where organisations refine and optimise their practices through the use of tools like password managers and the activation of account alerts; and finally, Mastery, where the highest level of security practices, including password hashing and regular audits, are fully integrated into the organisation's culture and processes. These themes represent a structured progression from initial awareness to the ultimate mastery of password security practices, providing a clear and comprehensive pathway for organisations to systematically improve their cybersecurity education and posture.

5. Password Security Education Maturity Model

The proposed Password Security Education Maturity Model (PSEMM) provides a structured, progressive approach for organizations to cultivate robust password security practices through five key stages: Naivety, Foundational Awareness, Active Engagement, Embedded Security Habits, and an Adaptive Security Mindset. Each stage builds upon the last, enhancing the depth and effectiveness of password security measures, from initial awareness to an instinctive, adaptive approach. Progression through these stages strengthens the organization's collective security posture, integrating secure practices into both individual behaviour and organizational culture.

The Password Security Engagement and Proficiency Model (PSEPM) guides organizations through five stages to build a strong, adaptive password security culture. Starting with Foundational Awareness, employees gain basic knowledge of password security and common threats. In Active Engagement, they take ownership of security practices through hands-on training and personal security scorecards. At the Embedded Security Habits stage, secure practices become second nature, reinforced by ongoing reminders and peer support. Finally, the Adaptive Security Mindset stage fosters a proactive approach, where employees instinctively adjust to new security threats and integrate security into daily problem-solving. This model cultivates a resilient, security-conscious culture that evolves with emerging challenges.

At the Awareness level, emphasis is placed on cultivating the knowledge base of employees regarding the critical significance of password security and fundamental best practices, encompassing aspects such as ensuring sufficient length and complexity, as well as recognising prevalent threats like phishing and password cracking (Thomas, 2018). This phase underscores the indispensable need for organisations to establish a foundational understanding of password security among their employees.

Progressing to the Implementation level, organisations commence the application of their fundamental knowledge by deploying unique passwords for all accounts, enabling two-factor authentication (2FA), and securely storing passwords through tools like password managers. The primary objective is to ensure the consistent implementation of these rudimentary security measures across the organisation, thereby fostering a more secure environment and mitigating the risks associated with weak or reused passwords (Maralbayev et al., 2023)

The Enhancement level entails the adoption of more advanced password security measures, such as the utilisation of passphrases in lieu of single words, the integration of multi-factor authentication (MFA), and the periodic updating and rotation of passwords. These practices furnish an additional stratum of security, rendering it more arduous for malefactors to gain unauthorised access (Gundu, 2023).

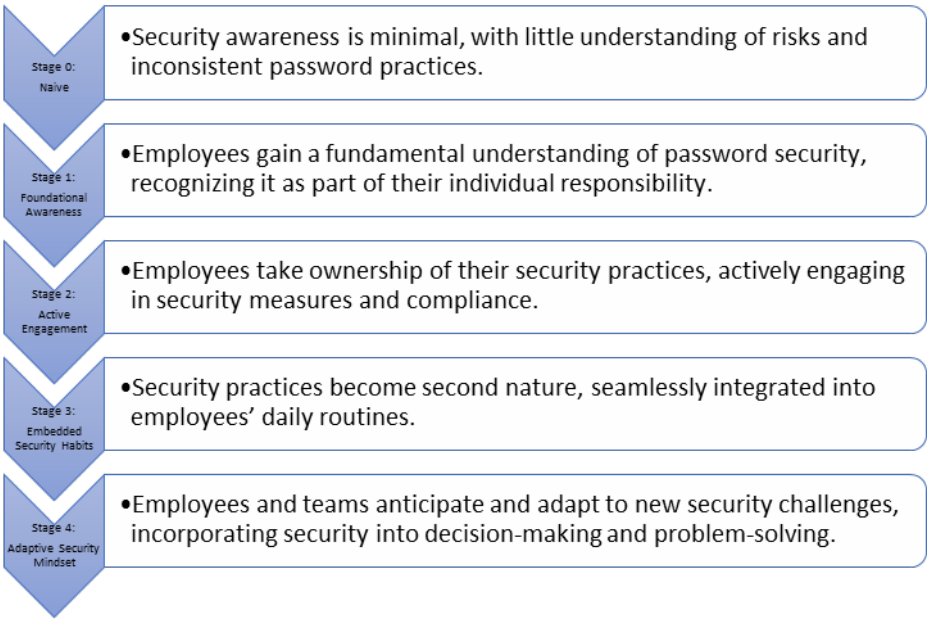

Figure 2: Password Security Education Maturity Model (PSEMM)

In **Stage 0: Naive**, the organization operates with minimal security awareness. Passwords are often weak and reused, and there is no formal training or clear policies in place. Security tools like password managers are not

widely adopted, leaving the organization vulnerable to security breaches. At this stage, the goal is to establish foundational awareness of password security and introduce basic tools and guidelines.

In **Stage 1: Foundational Awareness**, employees begin to understand the significance of password security as a personal responsibility. Initial training sessions cover basic risks, such as phishing, and introduce essential practices. Password managers are provided to store passwords securely, and departments designate "Cybersecurity Advocates" to promote security best practices. By the end of this stage, employees have a fundamental understanding of password security, recognizing it as an important aspect of their role.

Progressing to **Stage 2: Active Engagement**, employees transition from passive awareness to active participation in security practices. They undergo regular training sessions, including simulations and interactive exercises, which reinforce secure behaviour. Personal security scorecards are introduced, allowing employees to track their compliance and motivating them to take responsibility for their security practices. Password managers are fully utilized, not just for storage but also for generating strong, unique passwords. At this stage, employees demonstrate a high level of engagement with security, embracing password hygiene as a part of their routine.

By **Stage 3: Embedded Security Habits**, secure behaviours have become second nature to employees. Security practices are repeated so frequently that they become automatic, reducing the mental load associated with maintaining good password habits. Short, recurring micro-trainings and reminders, such as monthly tips or guidance during logins, keep these practices fresh and integrated into daily routines. Security champions within departments support and reinforce these habits, while recognition programs highlight consistent security efforts, celebrating employees and teams who excel in maintaining secure practices. At this stage, employees treat security as instinctual, fostering a naturally secure environment where secure behaviours are woven into the fabric of the organization.

Finally, in **Stage 4: Adaptive Security Mindset**, the organization achieves a state where employees and teams instinctively anticipate and adapt to emerging security challenges. Security awareness is proactive, with regular updates on new threats like AI-driven attacks and social engineering integrated into everyday workflows. Teams periodically review and refine their security practices to ensure they align with the latest cybersecurity developments, treating adaptation as a seamless part of their responsibilities. Employees exhibit a flexible approach to security, rapidly adjusting to new threats or incidents as they arise. Security discussions become a regular part of team meetings and strategic planning sessions, fostering an adaptive security mindset that is ingrained in the organization's culture. By the end of this stage, the organization maintains a resilient, forward-thinking security posture, equipped to handle evolving threats through a continuous commitment to proactive security.

6. Discussion

Although PSEMM can ensure that organizations can systematically build upon their existing practices, fostering continuous improvement, it also has certain limitations. For example, the model's complexity, particularly in the later stages of Optimization and Mastery, may pose challenges for smaller organizations with limited resources and limited IT capabilities. The resource-intensive nature of these stages could hinder the ability of some organizations to fully implement the model. Furthermore, while the PSEMM's focus on password security provides depth, it may lack the broader applicability of existing models that address overall cybersecurity or information security maturity. This specialization, while beneficial for targeted improvements, might limit its integration into a wider cybersecurity strategy meaning that organizations seeking a more holistic security model may need to supplement the PSEMM with other frameworks to cover all aspects of their cybersecurity needs.

Another significant challenge is gaining organisational buy-in, particularly from management and employees who may not immediately see the value in adopting a structured maturity model. Resistance to change is a common issue, especially in organisations that do not have a strong culture of continuous improvement or security awareness.

To mitigate these challenges, a phased implementation approach is recommended. Organisations can gradually roll out the model's practices, aligning them with available resources and capabilities. This allows for incremental progress and reduces the strain on resources. Additionally, careful planning of resource allocation, potentially involving external support or partnerships, can help organisations navigate the more resource-intensive stages of the model.

7. Conclusion

The Password Security Engagement and Proficiency Model (PSEPM) provides a progressive approach to establishing a resilient password security culture within organizations. Unlike traditional models, the PSEPM focuses on embedding security practices into the daily lives and mindsets of employees, gradually moving from foundational knowledge to an adaptive security mindset. Starting with Naivety then Foundational Awareness, the model builds an essential knowledge base that grows into Active Engagement, where employees take responsibility for their security practices. This engagement deepens into Embedded Security Habits, ensuring that secure behaviours become instinctive parts of employees' routines. Ultimately, the Adaptive Security Mindset stage equips the organization with a proactive, resilient approach to emerging threats, where employees intuitively integrate security into their daily work and problem-solving processes.

Practitioners should prioritise securing management buy-in by clearly communicating the long-term benefits of the model. Tailoring the educational components to the specific needs of different employee groups will enhance engagement and effectiveness. It is also advisable to establish metrics for assessing progress at each stage of the model, allowing for continuous monitoring and adjustment. Organisations should consider leveraging external expertise or partnerships, especially when advancing to the more resource-intensive stages of Optimisation and Mastery.

The adoption of the PSEMM has the potential to significantly elevate organisational cybersecurity practices by embedding a structured, education-driven approach to password security. By systematically improving password security education and practices, organisations can reduce their vulnerability to cyberattacks and foster a culture of continuous improvement in cybersecurity. The PSEMM not only bridges the gap between theory and practice but also sets a new standard for how organisations approach password security in an increasingly digital world.

Future direction leans towards conducting longitudinal case studies in a selection of organizations to observe the long-term impact of implementing the PSEMM. Future research will focus on how the model affects organizational behavior, security posture, and overall resilience to cyber threats over time.

AI Declaration: Artificial Intelligence (AI) tools were used solely for language refinement. All intellectual contributions, analyses, and conclusions were developed by the authors, with AI serving only as a supplementary aid for clarity and readability. No AI-generated content was included without human oversight and critical review.

Ethics Declaration: This research did not require ethical clearance as it did not involve human participants, personal data, or any activities that posed ethical concerns. However, all research activities were conducted in accordance with ethical principles, including academic integrity, responsible data management, and adherence to best practices in research ethics.

References

Alqahtani, M.A., 2022. Factors Affecting Cybersecurity Awareness among University Students. Appl. Sci. 12, 2589. https://doi.org/10.3390/app12052589

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A., Akin, E., 2023. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 12, 1333. https://doi.org/10.3390/electronics12061333

Bashorun, A., Worwui, A., Parker, D., 2013. Information security: To determine its level of awareness in an organization, in: 2013 7th International Conference on Application of Information and Communication Technologies. Presented at the 2013 7th International Conference on Application of Information and Communication Technologies, pp. 1–5. https://doi.org/10.1109/ICAICT.2013.6722704

Bauer, S., Bernroider, E., Chudzikowski, K., 2013. End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study.

Bhana, B., Flowerday, S.V., 2021. Usability of the login authentication process: passphrases and passwords. Inf. Comput. Secur. 30, 280–305. https://doi.org/10.1108/ICS-07-2021-0093

Bitwarden, 2025. Password Management Maturity Model [WWW Document]. URL https://bitwarden.com/resources/password-management-maturity-model/

Chatzoglou, E., Kampourakis, V., Tsiatsikas, Z., Karopoulos, G., Kambourakis, G., 2024. Keep your memory dump shut: Unveiling data leaks in password managers. https://doi.org/10.48550/arXiv.2404.00423

Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., Ofusori, L., Ome, U., 2023. Password-based authentication and the experiences of end users. Sci. Afr. 21, e01743. https://doi.org/10.1016/j.sciaf.2023.e01743

Farshim, P., Tessaro, S., 2021. Password Hashing and Preprocessing, in: Canteaut, A., Standaert, F.-X. (Eds.), Advances in Cryptology – EUROCRYPT 2021. Springer International Publishing, Cham, pp. 64–91. https://doi.org/10.1007/978-3-030-77886-6_3

Gundu, T., 2024. Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model. Int. Conf. Cyber Warf. Secur. 19, 95–102. https://doi.org/10.34190/iccws.19.1.2177

Gundu, T., 2023. Enhancing Remote Work Security: A Multi-Key Biometric Authentication Scheme for Virtual Workspaces, in: 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET). pp. 1–7. https://doi.org/10.1109/ICECET58911.2023.10389214

Gundu, T., Modiba, N., 2020. Building Competitive Advantage from Ubuntu: An African Information Security Awareness Model., in: ICISSP. pp. 569–576.

Hein-Pensel, F., Winkler, H., Brückner, A., Wölke, M., Jabs, I., Mayan, I.J., Kirschenbaum, A., Friedrich, J., Zinke-Wehlmann, C., 2023. Maturity assessment for Industry 5.0: A review of existing maturity models. J. Manuf. Syst. 66, 200–210. https://doi.org/10.1016/j.jmsy.2022.12.009

Hu, S., Hsu, C., Zhou, Z., 2022. Security Education, Training, and Awareness Programs: Literature Review. J. Comput. Inf. Syst. 62, 752–764. https://doi.org/10.1080/08874417.2021.1913671

Huang, Z., Bauer, L., Reiter, M.K., 2024. The Impact of Exposed Passwords on Honeyword Efficacy. Presented at the 33rd USENIX Security Symposium (USENIX Security 24), pp. 559–576.

Hussey, K., 2024. Secure Access Control Maturity [WWW Document]. URL https://www.tditechnologies.com/2024/01/16/identity-and-secure-remote-access-control/ (accessed 3.23.25).

Hussey, K., 2021. Password Management Maturity Model [WWW Document]. URL https://www.tditechnologies.com/2021/11/09/password-management-maturity-model/ (accessed 3.23.25).

Juozapavičius, A., Brilingaitė, A., Bukauskas, L., Lugo, R.G., 2022. Age and Gender Impact on Password Hygiene. Appl. Sci. 12, 894. https://doi.org/10.3390/app12020894

Keeper, 2025. Meet CMMC Requirements with Keeper Security [WWW Document]. URL https://www.keepersecurity.com/cmmc/

Khan, B., Alghathbar, K., Nabi, S., Khan, K., 2011. Effectiveness of information security awareness methods based on psychological theories. Afr. J. Bus. Manag. 5. https://doi.org/10.5897/AJBM11.067

Lasrado, L.A., Vatrapu, R., Andersen, K.N., n.d. Maturity Models Development in IS Research: A Literature Review.

Maralbayev, A., Omar, G.-S., Abdulayeva, M., Rzayeva, L., Kalybek, G., Rakhym, E., 2023. New Algorithm of Weak Password Detection, in: 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM). Presented at the 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 1–6. https://doi.org/10.1109/WINCOM59760.2023.10323000

Muronga, K., Herselman, M., Botha, A., Da Veiga, A., 2019. An Analysis of Assessment Approaches and Maturity Scales used for Evaluation of Information Security and Cybersecurity User Awareness and Training Programs: A Scoping Review, in: 2019 Conference on Next Generation Computing Applications (NextComp). Presented at the 2019 Conference on Next Generation Computing Applications (NextComp), pp. 1–6. https://doi.org/10.1109/NEXTCOMP.2019.8883535

Oesch, S., Ruoti, S., Simmons, J., Gautam, A., 2022. "It Basically Started Using Me:" An Observational Study of Password Manager Usage, in: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, CHI '22. Association for Computing Machinery, New York, NY, USA, pp. 1–23. https://doi.org/10.1145/3491102.3517534

Rabii, A., Assoul, S., Ouazzani Touhami, K., Roudies, O., 2020. Information and cyber security maturity models: a systematic literature review. Inf. Comput. Secur. 28, 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Sauer, P.C., Seuring, S., 2023. How to conduct systematic literature reviews in management research: a guide in 6 steps and 14 decisions. Rev. Manag. Sci. 17, 1899–1933. https://doi.org/10.1007/s11846-023-00668-3

Siponen, M., Adam Mahmood, M., Pahnila, S., 2014. Employees' adherence to information security policies: An exploratory field study. Inf. Manage. 51, 217–224. https://doi.org/10.1016/j.im.2013.08.006

Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R., Shabtai, A., 2022. Contextual security awareness: A context-based approach for assessing the security awareness of users. Knowl.-Based Syst. 246, 108709. https://doi.org/10.1016/j.knosys.2022.108709

Thomas, J., 2018. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks.

Verizon 2024 DBIR, n.d. DBIR Report 2024 - Summary of Findings [WWW Document]. Verizon Bus. URL https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/ (accessed 9.2.24).

Yeo, K.T., Ren, Y., 2009. Risk management capability maturity model for complex product systems (CoPS) projects. Syst. Eng. 12, 275–294. https://doi.org/10.1002/sys.20123

Zluri, 2024. Identity & Access Management Maturity Model - A Guide for 2025 [WWW Document]. URL https://www.zluri.com/blog/identity-and-access-management-maturity-model (accessed 1.23.25).