Social Media and Enterprise Password Reuse Problem: Password Security Guidelines for Manufacturing Enterprises

Georgia Barnard and Tapiwa Gundu
Nelson Mandela University, Gqeberha, South Africa

tapgun@gmail.com

Abstract. The widespread use of the same passwords for social media and enterprise accounts presents a significant risk to organisational security. Through social engineering attacks such as phishing, hackers can try and gain information from users, using this information to try and guess your password to your social media accounts and attempt to see whether it is the same for your enterprise account. This study aims to create campaign guidelines for raising awareness amongst social media users about password security. The following Secondary Research Objectives have been used to aid the Research Question. Secondary Research Objective 1

(SRO1) was to assess security risks, preventive measures, best practices, and challenges related to password reuse across various platforms. Secondary Research Objective 2 (SRO2) aimed to identify key elements for successful password security campaigns. Using these Secondary Research objectives, we will be able to address the Research Question and apply critical reasoning to come up with guidelines that can help users learn about password security and raise awareness about safe password security practices. In essence, the study emphasises a layered approach that combines strong policies, user education, and balanced usability to enhance password security effectively. Through these efforts, this study aims to develop personalised social media campaign guidelines to improve employee's understanding of password security, encouraging a culture of proactive cybersecurity practices and safeguarding organisational data.

Keywords: Password Security, Social Media, Awareness Campaigns, Cybersecurity Education, Employee Awareness.

1. Introduction

Passwords are essential for securing both personal and professional accounts, serving as primary access credentials for various systems, applications, and devices. The structure of an effective password—typically a mix of characters, numbers, and symbols—intends to minimise unauthorised access. However, the repetitive creation and management of multiple passwords across platforms can lead to “password fatigue,” a major reason for risky practices like password reuse (Juozapavičius et al., 2022). In the case of social media, where security protocols are often less stringent than in corporate environments, users may unknowingly expose both personal and work accounts to exploitation (Aichner et al., 2021).

Phishing and social engineering are common attack methods leveraged on social media, where attackers extract non-sensitive personal information to deduce or guess users’ passwords. Such information can then be used to compromise accounts with reused credentials, facilitating unauthorised access to enterprise systems. Studies underscore that an integrated approach combining multi-factor authentication (MFA), regular password updates, and cybersecurity training can counteract these risks effectively by enhancing user awareness and password hygiene (Chaudhary et al., 2019; Jain et al., 2021). Thus, creating distinct, complex passwords for each account, paired with awareness initiatives, is crucial in minimizing vulnerabilities arising from password reuse.

1.1 Social Media and Password Security

As the use of social media is becoming increasingly intertwined with daily life, employees inadvertently expose themselves and their organizations to the threat of cyber-attacks. For instance, access to personal and work accounts on social media tends to be so convenient that caution is thrown to the wind, hence the possibility of successful phishing attacks. According to Alharbi et al. (2022), employees also tend to reuse the same passwords across accounts. The transition to working from home, for example, during the COVID-19 pandemic increased the usage of personal devices, which supposedly may not be as tightly controlled in terms of security controls compared to enterprise devices. The trend has increased the need for security awareness among employees, especially for organizations that depend on employees' access to social media or online resources to operate.

Effective security awareness programs educate employees on recognizing and avoiding threats, like phishing and social engineering. They emphasize the need for unique passwords for each account and the role of privacy settings in managing personal data exposure (Ifpo, 2010; Khando et al., 2021). These programs are essential in manufacturing enterprises, where shared networks and third-party application integrations are common, creating additional security concerns (Aslan et al., 2023). By promoting a culture of security awareness,

organizations can empower employees to maintain secure practices, thus reinforcing both individual and organizational defences against cyber threats.

1.2 Manufacturing Enterprise

Password protection and cybersecurity threat awareness among employees are gradually gaining importance in the manufacturing sectors as most of them are adopting digital manufacturing processes and systems connected over the Internet. Manufacturing enterprises have frequently been at the receiving end of unique security challenges as their operations depend on operational technologies that are less adaptable to frequent password changes or multi-factor authentication due to operational constraints (Chaudhary et al., 2019). Employees frequently access a mix of personal and work-related accounts on the same network, increasing the likelihood of password reuse across social media and enterprise systems (Jain et al., 2021). The result is that critical production and intellectual property data then become highly vulnerable, as even unauthorised access to one weakness disrupts the operational networks of an organisation.

Not to mention general password reuse risks, manufacturing companies quite often provide third party applications with access to supply chain and production management, hence adding more vulnerability to credential-based attacks. Breaches of social media or phishing attacks on employees' accounts result in unnoticed access to critical systems due to password reuse (Alharbi et al., 2022). Thus, comprehensive training programs in password hygiene, multi-factor authentication, and cautious social media usage must be prioritized by a manufacturing organization. In turn, this would

protect operational continuity and security.

1.3 Research Objectives

The primary objective centres on creating awareness campaign guidelines aimed at educating social media users on password security. To support this goal, the secondary objectives explore distinct areas of research, from evaluating existing literature to gathering empirical data on user behaviour and awareness.

Primary Research Objective (PRO): To create campaign guidelines for raising awareness among social media users about password security.

Secondary Research Objective 1 (SRO1): Conducted a literature review to assess prevalent security risks, best practices, and challenges related to password reuse across different platforms.

Secondary Research Objective 2 (SRO2): Through a systematic literature review to assess security risks, preventive measures, best practices, and challenges related to password reuse across various platforms.

The remainder of this paper is structured as follows: Section 2 details the methodology used to construct the Password Security Awareness Guidelines, including the systematic literature review and criteria selection processes. In Section 3 and 4, the research findings are outlined and discussed. Section 5 presents the proposed guidelines. Finally, Section 6 concludes the paper by summarising the key findings, outlining future research directions.

2. Methodology

This study employed a systematic literature review (SLR). A Systematic Literature Review (SLR) is a rigorous academic procedure that systematically examines, assesses, and combines research in an impartial manner relating to a particular field or topic. The review is designed to be thorough, clear, and replicable compared to traditional narrative reviews. The principle of SLR is to minimise bias and enhance the credibility of results through a structured approach to conducting literature reviews. This approach assists researchers in making conclusions about the status of research on a particular question or topic. SLRs are valuable for identifying gaps in research, compiling empirical evidence, and developing theoretical frameworks for upcoming studies. It was constructed in various phases that flow seamlessly from one to the next.

2.1 SLR Process

The Systematic Literature Review (SLR) process for this study is structured to ensure a comprehensive, unbiased selection of literature relevant to the research question, "What are the key elements that contribute to effective password security initiatives?" This systematic approach is essential to understanding different aspects of

password security, including policy frameworks, multi-factor authentication, user behaviour, and password complexity by analysing the latest studies in the field. The SLR aims to produce well-supported, evidence-based insights into best practices for enhancing password security in organizational contexts.

The SLR process, illustrated in Figure 2.1, begins with an extensive search across reputable databases: Google Scholar, ScienceDirect, and ResearchGate. Using search terms such as "password" and "password in security," the initial search yielded 122 studies. There was 113 from Google Scholar, 5 from ScienceDirect, and 3 from ResearchGate. This wide-ranging search is designed to capture a broad array of perspectives on password security, ensuring that the dataset is comprehensive and relevant.

The first filtering step, Primary Screening and Filtering applies specific inclusion criteria to the initial dataset. Only studies published in English, within the years 2021 to 2024, are considered to ensure the review focuses on recent findings applicable to modern security challenges. This primary screening eliminates 73 studies that do not meet these standards, reducing the pool to 40 studies that align more closely with the study's organizational focus. Following this, Duplicate Removal is performed to ensure each study in the dataset is unique. This step removes 10 redundant entries, leaving 40 studies for further analysis. This refinement helps ensure that each selected study provides original content without repetition, making the dataset more efficient for the subsequent stages.

The Secondary Screening for Relevance involves a more detailed evaluation of the remaining 40 studies. Titles, abstracts, and keywords are reviewed to determine each study's direct relevance to the research objective, which is focused on password security initiatives within organizations. Studies that do not specifically address this context are excluded, narrowing the selection to 10 studies that more accurately reflect the study's goals.

These 10 studies then enter the Shortlisting for Final Review stage, where each study undergoes a rigorous review to confirm it contains substantial empirical data or in-depth evaluations of password security strategies. Studies that lack the necessary empirical focus are excluded, leaving a final, refined set of 10 studies that offer the most relevant insights for the research.

The Final Selection and Inclusion step concludes the SLR process, establishing a core set of 10 studies that provide the most robust evidence and valuable insights into effective password security practices. This selected body of literature serves as a strong foundation for subsequent analysis, helping to identify best practices and inform the development of security guidelines. Through each carefully structured stage, as outlined in Figure 1, the SLR process progressively refines the literature set, ensuring a focused and reliable basis for synthesizing findings and advancing password security research, these papers were compiled in Table 1.

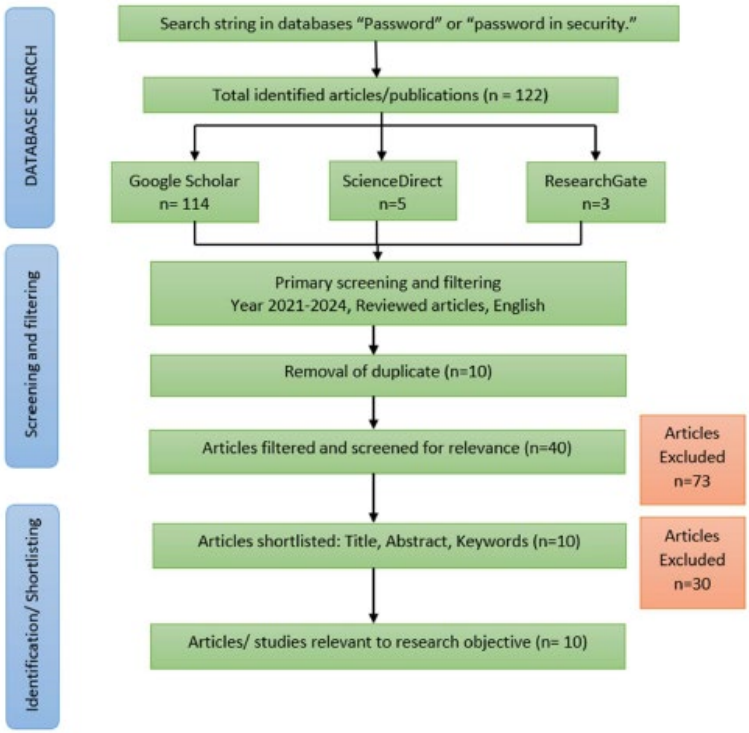

Figure 1: Systematic Literature Review Process

3. Findings

The Analysis Results showcase the main discoveries of the chosen studies in the SLR database, emphasising central topics related to password security in enterprises as seen in Table 1. The themes identified are password complexity, user education, password management tools, security policy adherence, and balancing user convenience and security.

Table 1: Themes identified through SLR

Theme	Articles
Password Complexity Requirements	(Lee et al., 2022); (Shin and Woo, 2022)
User Education and Awareness	(Kanta et al., 2020); (Guo et al., 2020)
Password Management Tools	(Chaudhary et al., 2019);(Tian, 2024)
Security Policies and Compliance	(Lee et al., 2022); (Chakraborty et al., 2022)
User Convenience vs. Security	(Atzori et al., 2024); (Thomas et al., 2019)

4. Discussion

Understanding password security is crucial for manufacturing enterprises, given the increasing cyber threats targeting industrial systems. This study investigated the existing password security practices, highlighting critical gaps and areas for improvement. This section discusses the themes identified through the SLR in detail.

4.1 Password Complexity Requirements

Password complexity requirements, as proposed by two seminal articles, are primarily concerned with the principles and criteria that dictate the minimum level of difficulty that a password must have to offer robust security, according to Lee et al. (2022), in their study, "Password policies of most top websites fail to follow best practices," they critically examine the password policies that are currently in place on well-known websites, highlighting the differences between suggested standards and actual implementation. Complementing this, Shin & Woo (2022), in "PasswordTensor: Analysing and explaining password strength using tensor decomposition," presents a fresh analytical approach to determining the strength of a password. Their study sheds more light on the best way to construct complex passwords to thwart attempts at cracking them and improve overall security.

4.2 User Education and Awareness

To prevent breaches and ensure best practices are followed, users must be taught about password security. Two papers address this subject. Kanta et al. (2020), in "A survey exploring open source Intelligence for smarter password cracking," highlights the weaknesses that result from inadequate user awareness. Their research highlights how advanced password-cracking methods take advantage of these ignorance gaps, highlighting the significance of user education. Meanwhile, Guo et al. (2020), in "Nudging personalized password policies by understanding users' personality," suggest that adjusting password policies to suit the individual personalities of users can improve the efficacy of training. By considering user behaviour, security measures can be tailored to be more successful in promoting secure habits and engaging users.

4.3 Password Management Tools

For users to manage their credentials securely and conveniently, password management tools are essential. This subject is covered in two papers. For users to manage their credentials securely and conveniently, password management tools are essential. This subject is covered in two papers. Chaudhary et al. (2019), in their study "Usability, security, and trust in password managers: A quest for user-centric properties and features," Look at the delicate balance between security and usability found in password managers. They emphasize how important it is to design these technologies with user-centric features in mind to boost confidence and acceptance. Similarly, Tian. (2024), in "Unraveling the dynamics of password manager adoption: a deeper dive into critical factors," investigates the factors influencing the use of password managers. This study provides recommendations on how to increase users' adoption of these technologies by illuminating the factors influencing their choices to accept or reject them.

4.4 Security Policies and Compliance

Strict adherence to security policy and industry standards is necessary to ensure password protection. Two studies support this idea further. As previously noted, Lee et al. (2022), also belong to this group since they raise doubts about the extent to which password rules follow recognised best practices. Their research identifies significant flaws in current policies and advocates for their modification. Additionally, Chakraborty et al. (2022) provide a comprehensive overview of honeyword-based strategies in "Honeyword-based Authentication Techniques for Protecting Passwords: A Survey." By ensuring that authentication processes adhere to stringent security guidelines and protect users from potential threats, these solutions aim to improve password security.

4.5 User Convenience vs. Security Trade-offs

A key challenge in password management is finding a balance between user convenience and security. Two papers address this problem. Thomas et al. (2019), discuss the challenge of safeguarding users against credential stuffing attacks without compromising usability in their article, "Protecting accounts from credential stuffing with password breach alerting." They stress how important it is to find a balance between offering robust security and ease of use. In a similar context, Atzori et al. (2024), explore in "Evaluating password strength based on information spread on social networks: A combined approach relying on data reconstruction and generative models" how data from social networks might be used to assess and enhance password strength. Their approach is to provide a method that is both safe and simple to use by striking a balance between the needs for simplicity and security.

5. Proposed Password Security Guidelines or Manufacturing Enterprises

To enhance cybersecurity within manufacturing enterprises, it is essential to establish clear guidelines on password security. Table 2 outlines key recommendations that organizations should implement to strengthen password policies, educate users, promote secure password management, and maintain a balance between security and usability. These guidelines are directly informed by the findings of the study, which highlighted common weaknesses in password policies, the effectiveness of user education, the role of password management tools, and the challenges of balancing security with user convenience. By adopting these best practices, enterprises can mitigate security risks and improve overall cyber resilience.

Table 2: Password Security Guidelines or Manufacturing Enterprises

Guideline	Description
Enforce Strong Password Complexity Requirements	• Establish policies requiring a mix of uppercase and lowercase letters, numbers, and special characters. • Set a minimum password length (e.g., at least 12 characters). • Regularly review and update password policies to align with best practices. • Implement password strength analysis tools to enforce complexity.
Conduct Regular User Education and Awareness Campaigns	• Provide ongoing training on password security and common threats like phishing and social engineering. • Customize training programs to consider user behaviours and personality traits. • Use real-world case studies to demonstrate the risks associated with weak passwords. • Reinforce security habits through interactive learning and simulations.
Promote the Use of Password Management Tools	• Encourage employees to use password managers for secure storage and generation of strong passwords. • Select password managers that balance security and ease of use. • Provide guidelines on choosing reputable password managers and avoiding unsafe storage practices. • Regularly assess adoption rates and address concerns regarding usability and trust.
Implement Robust Security Policies and Compliance Measures	• Enforce organization-wide security policies that align with industry standards. • Conduct regular audits and updates to address emerging threats.

Guideline	Description
	• Consider implementing honeyword-based authentication to enhance security. • Ensure compliance with data security regulations and best practices.
Balance User Convenience and Security Effectively	• Implement security measures that protect against credential-stuffing attacks while maintaining usability. • Encourage the use of multi-factor authentication (MFA) for added security. • Leverage AI-driven techniques to evaluate and improve password strength. • Continuously assess security protocols to ensure a balance between ease of use and protection.

6. Conclusion

This study contributes significantly to the understanding and promotion of password security awareness in the manufacturing sector by establishing a structured approach to campaign guidelines tailored to this industry. This research points out the risks due to password reuse and social media as an educational platform for effective motivation of people towards the core issue presented in the problem statement: organisational data are in danger because the employees use the same passwords both for personal and professional accounts. In such a context, the study performs a critical review of the related literature and hence offers a systematic review, which points out those aspects that have been hindering password hygiene, including password fatigue, a lack of awareness, and convenience regarding password reuse.

These insights form the basis for achieving the primary research objective (PRO), the creation of campaign guidelines aimed at enhancing password security awareness. The study offers a foundation for developing targeted messaging strategies that resonate with manufacturing employees, whose roles often involve interactions across both social media and enterprise systems. It emphasises practical elements like multi-factor authentication (MFA), password management tools, and regular cybersecurity education, which are essential to fostering secure password practices and addressing the unique cybersecurity challenges in manufacturing environments.

Additionally, by outlining awareness strategies that incorporate both behavioural and technological recommendations, the study supports the manufacturing sector's need for a culture of proactive cybersecurity. This approach aligns with the problem statement by proposing actionable steps that can help prevent unauthorised access and safeguard critical organisational data. In doing so, the study not only addresses immediate password security issues but also lays the groundwork for future, data-driven campaigns that can further reinforce security awareness among employees. These contributions enhance the manufacturing sector's resilience against cyber threats and provide a scalable model for password security campaigns that could be applied in other industries facing similar challenges.

Future studies should explore the practical implementation of the proposed campaign guidelines within manufacturing enterprises, evaluating the effectiveness of different awareness raising methods, such as training sessions, visual reminders, and interactive workshops, in improving password security practices. Implementing and testing the guidelines in real-world settings would allow for adjustments based on feedback and observed outcomes, further refining the approach to meet the unique security needs of the manufacturing sector. This next phase of research would help ensure that the guidelines not only align with best cybersecurity practices but also resonate with and positively impact employees' behaviour in protecting both personal and corporate accounts.

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.

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.

References

Aichner, T., Grünfelder, M., Maurer, O., Jegeni, D., 2021. Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019. Cyberpsychology, Behavior, and Social Networking 24, 215–222. https://doi.org/10.1089/cyber.2020.0134

Alharbi, A., Alotaibi, A., Alghofaili, L., Alsalamah, M., Alwasil, N., Elkhediri, S., 2022. Security in Social-Media: Awareness of Phishing Attacks Techniques and Countermeasures, in: 2022 2nd International Conference on Computing and Information Technology (ICCIT). Presented at the 2022 2nd International Conference on Computing and Information Technology (ICCIT), pp. 10–16. https://doi.org/10.1109/ICCIT52419.2022.9711640

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

Atzori, M., Calò, E., Caruccio, L., Cirillo, S., Polese, G., Solimando, G., 2024. Evaluating password strength based on information spread on social networks: A combined approach relying on data reconstruction and generative models. Online Social Networks and Media 42, 100278. https://doi.org/10.1016/j.osnem.2024.100278

Chakraborty, N., Li, J., Leung, V.C.M., Mondal, S., Pan, Y., Luo, C., Mukherjee, M., 2022. Honeyword-based Authentication Techniques for Protecting Passwords: A Survey. ACM Comput. Surv. 55, 169:1-169:37. https://doi.org/10.1145/3552431

Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M., Berki, E., 2019. Usability, security and trust in password managers: A quest for user-centric properties and features. Computer Science Review 33, 69–90. https://doi.org/10.1016/j.cosrev.2019.03.002

Guo, Yimin, Zhang, Z., Guo, Yajun, Guo, X., 2020. Nudging personalized password policies by understanding users' personality. Computers & Security 94, 101801. https://doi.org/10.1016/j.cose.2020.101801

Ifpo (Ed.), 2010. Chapter 7 - Security Awareness, in: The Professional Protection Officer. Butterworth-Heinemann, Boston, pp. 83–88. https://doi.org/10.1016/B978-1-85617-746-7.00007-9

Jain, A.K., Sahoo, S.R., Kaubiyal, J., 2021. Online social networks security and privacy: comprehensive review and analysis. Complex Intell. Syst. 7, 2157–2177. https://doi.org/10.1007/s40747-021-00409-7

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

Kanta, A., Coisel, I., Scanlon, M., 2020. A survey exploring open source Intelligence for smarter password cracking. Forensic Science International: Digital Investigation 35, 301075. https://doi.org/10.1016/j.fsidi.2020.301075

Khando, K., Gao, S., Islam, S.M., Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security 106, 102267. https://doi.org/10.1016/j.cose.2021.102267

Lee, K., Sjöberg, S., Narayanan, A., 2022. Password policies of most top websites fail to follow best practices. Presented at the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022), pp. 561–580.

Shin, Y., Woo, S.S., 2022. PasswordTensor: Analyzing and explaining password strength using tensor decomposition. Computers & Security 116, 102634. https://doi.org/10.1016/j.cose.2022.102634

Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Kelley, P.G., Invernizzi, L., Benko, B., Pietraszek, T., Patel, S., Boneh, D., Bursztein, E., 2019. Protecting accounts from credential stuffing with password breach alerting. Presented at the 28th USENIX Security Symposium (USENIX Security 19), pp. 1556–1571.

Tian, X., 2024. Unraveling the dynamics of password manager adoption: a deeper dive into critical factors. Information & Computer Security ahead-of-print. https://doi.org/10.1108/ICS-09-2023-0156