Borneo International Journal eISSN 2636-9826; Vol. 7 (3); 2024; 49-58
Published by *Majmuah Enterprise*
www.majmuah.com

A Preliminary Study of Human Vulnerabilities in User Password Asset Management

SUREN KRISHNAN[1] and MASLINDA BINTI MOHD NADZIR[2]
[1]*Awang Had Salleh Graduate School, School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA*
[2]*School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA*
Email: surenkrishnan12@yahoo.com, maslinda@uum.edu.my | Tel: +601126532127, +601165109449 |

Received: August 27, 2024
Accepted: July 30, 2024
Online Published: Sept 02, 2024

Abstract

Human weaknesses often compromise effective user password management, posing serious hazards despite being a fundamental component of digital security. This study analyse human vulnerabilities in user password asset management. Reusing passwords and creating weak passwords are common factors examined. The study was conducted in three phases: planning, design and development, and data analysis. A questionnaire was distributed to 134 samples from an information technology organisation in Singapore. Statistical analysis of the survey identified key aspects contributing to these vulnerabilities, including human behaviour in password management practices. The examination of existing password practices indicates notable discrepancies that are impacted by user behaviour, underscoring the necessity of better policies and education to strengthen password security. The analysis highlights the influence of user behaviour, has on these methods' efficacy and shows how important human factors are to the security. The assessment of substitute authentication techniques has demonstrated that these technologies can significantly reduce cybersecurity risks associated with human interaction. Emerging issues in cybersecurity will require a combination of improved password restrictions, user education, and sophisticated user-friendly authentication techniques.

Keywords: password management, human vulnerabilities, password creation

1. Introduction

This chapter provides an overview of the study, detailing the problem statements, research questions, objectives, scope, and significance. Passwords are the cornerstones of digital security in today's interconnected world, serving as the main barrier against unwanted access to personal and organizational data. Human weaknesses in password management, despite their critical role, are a serious threat to digital security. User passwords are the frontline defense against unauthorised access to sensitive information, be it personal data, financial records, or valuable intellectual property. However, despite advancements in cybersecurity and the widespread awareness of password best practices, human vulnerabilities remain a critical concern in user password asset management. The usage of weak and simple-to-guess passwords presents a serious vulnerability. A National Institute of Standards and Technology (NIST) study found that 81% of data breaches were caused by leaked passwords, many of which were simple or common passwords like "123456" or "password" (Scarfone & Souppaya, 2009). This concerning figure emphasises how common this problem is and emphasises the need for stricter password policies. This is corroborated by the Verizon Data Breach Investigations Report (DBIR), which shows that 39% of breaches entail the usage of credentials that were lost or compromised (Verizon, 2023). These results highlight how important password strength is to overall security. Reusing the same password on several websites is another serious issue. According to a survey conducted in 2023 by the cybersecurity company Dashlane, 61% of people reuse their passwords across several accounts (Password Usage and Security Report, 2023).

Because of this approach, there is a cascading risk that is, if one account is compromised, attackers can use the compromised password to access other accounts, potentially doing even more damage. One important factor in password vulnerabilities is human mistake. According to an IBM X-Force study, human error including poor password management is to blame for 95% of cybersecurity breaches (IBM X-Force Threat Intelligence Index, 2022). Writing down passwords in public places or storing them insecurely in digital files that aren't encrypted or on paper notes, for example are common mistakes. These procedures increase the possibility of data breaches by giving unauthorised people simple access. The typical user maintains more than 90 passwords. This amount of password management can be overwhelming for users and encourage the adoption of unsafe password reuse or simple passwords. Users look for shortcuts because of this intricacy, which frequently jeopardises security. Despite the advancements in password security technologies, human vulnerabilities remain a significant factor contributing to the compromised security of user password assets (Alsharif, Mishra, & AlShehri, 2021). Businesses spend enormous sums of money installing security measures to prevent access to their systems because of the severe consequences of security breaches. Firewalls, authentication

systems, and other security measures have been implemented due to the increased investment (Tam, Glassman, & Vandenwauver, 2009). But even with these constant investments and efforts, there is one variable that money cannot buy: the user. Putting the user first is crucial because, despite improved authentication methods, businesses still frequently utilise password-based systems to manage system access. As a result, if users misuse their passwords, even the most advanced security system is rendered ineffective.



Figure 1: The importance of password security (The Importance of Password Security, 2024)

Based on a study by Clyrofor, 44% of users admitted to recycling passwords across personal and business-related accounts, increasing the risk of widespread security breaches. While 62% of users have shared a password over email or text messages, inadvertently exposing sensitive access credentials to potential interception. This shows that most users are unaware of the importance of password security. A password is a secret a claimant uses to verify its identity, usually a string of characters. One way to identify and authenticate oneself is to combine a password with a user identifier, like a username. The act of presenting an identifier that serves as a user identity for the system is known as identification. Establishing trust in the legitimacy of a claimant's provided identifier is the process of authentication, which is typically required before allowing access to resources in a system of information (Scarfone & Souppaya, 2009). It is considered knowledge of the password; if it is thought that only one person may know it, it identifies that person. Passwords are among the numerous little annoyances of technology and are pervasive in our day-to-day existence. Typically believe that, despite being annoying, passwords are also required to safeguard us from hackers and to identify people over large spaces, even if many businesses are working to find better ways to authenticate users in the globalised age of the Internet (Eve, 2016). For end users, creating secure, one-of-a-kind passwords for each account, keeping track of those passwords over time, and remembering which password is associated with which account across many accounts present significant usability challenges. Users are forced to design memorable but simple passwords for attackers to decode due to these security requirements, which make demands on their memory, time, and attention beyond human capacity (Stobert & Biddle, 2015). Although most users can memorise a few passwords easily, the recent surge in the number of passwords they must remember is seriously pushing the boundaries of their cognitive capacities. For instance, users frequently select short, "low entropy" passwords, which makes offline dictionary attacks and brute-forcing attempts possible. They also frequently write down their passwords or use the same password across several websites (Karole, Saxena, & Christin). However, organisations continue to face numerous challenges in this area, primarily due to human factors such as weak passwords, password reuse, and improper password management, which persist as significant vulnerabilities exploited by malicious actors (Otta, Panda, Gupta, & Hota, 2023). Studies have shown that individuals use easily predictable information, such as common words, personal names, or sequential numbers, in their passwords (Ugwu, et al., 2022). This behavior increases the likelihood of successful password-cracking attempts. Understanding these patterns of human behavior is crucial for developing interventions and tools that promote the creation of stronger, more secure passwords. Password managers are programs that use encryption to impose best practices for creating and protecting passwords (Ezugwu, et al., 2023). A password manager can be utilised to generate and store all of a user's passwords securely, with the assistance of a master password or key (Gangwal, Singh, & Srivastava, 2023). For enhanced security and convenience,

Borneo International Journal eISSN 2636-9826; Vol. 7 (3); 2024; 49-58
Published by *Majmuah Enterprise*
www.majmuah.com

password managers also offer the option of using biometric data, such as fingerprints or facial recognition, instead of a master password (Wang & Wang, 2022). By employing the password manager's built-in autofill feature, users can save time and reduce the likelihood of making input errors when filling in passwords and other information. Moreover, password managers enable users to share specific information with their trusted contacts without manually copying and pasting it into emails or instant messages. The structure is shown in Figure 2, and a detailed description of each step of the user password management lifecycle (Choong, 2014).

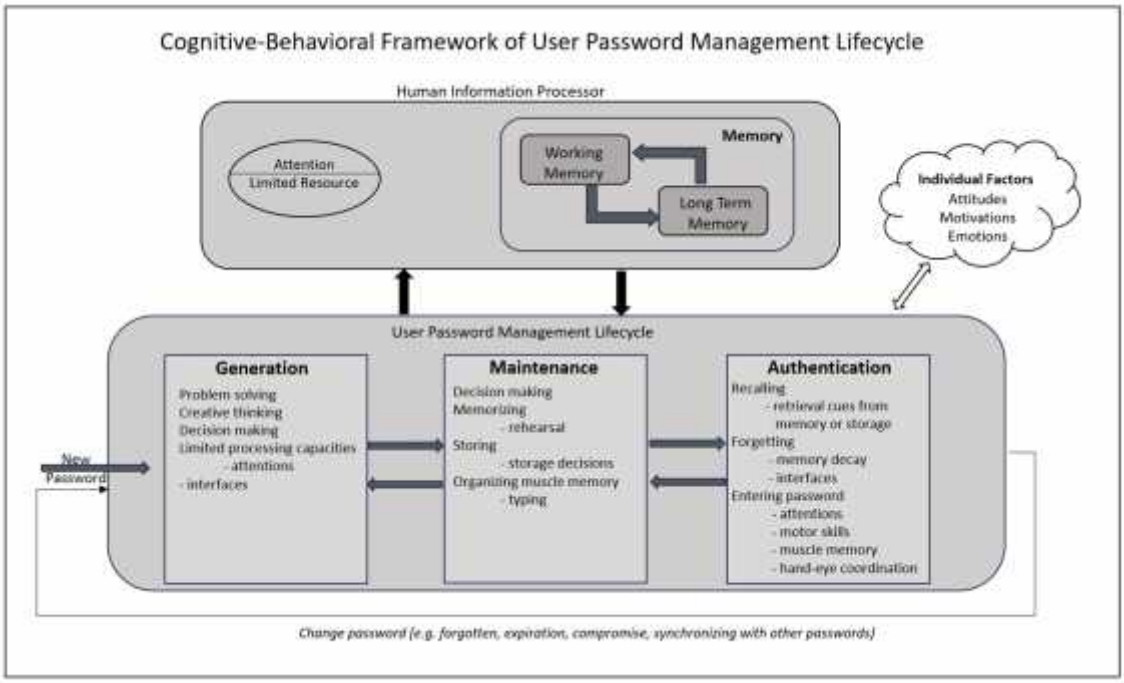

Figure 2: Cognitive-behavioral framework of user password management lifecycle

In the initial step of the password management lifecycle, called Generation, users must create a believable text string by joining different characters to meet the requirements for gaining access to the related account or system. The prerequisites, referred to as composition rules, are a popular organisational strategy used to get users to choose more secure passwords (Choong, 2014). During password creation, cognitive biases can influence human behavior and decision-making. These biases can impact users' password creation options, potentially leading to weaker security (Merdenyan & Petrie, 2022). Availability bias occurs when individuals rely on immediate examples or information that easily comes to mind. When creating passwords, users may be influenced by recent events or common patterns, leading to the use of predictable and easily predictable passwords. When making judgments, people often tend to place a lot of weight on the first piece of information they come across. In the context of password creation, users may anchor their choices based on familiar patterns or previously used passwords, leading to the reuse of passwords or the inclusion of personal information that can be easily associated with the user. Confirmation bias occurs when people seek or interpret information in a way that confirms their preexisting ideas or expectations (Alnifie & Kim, 2023). Regarding the generation of passwords, users may develop a sense of attachment or familiarity with their chosen passwords, making them resistant to changing or updating them, even if they are weak or compromised. The illusion of control bias occurs when individuals believe they have more control over outcomes than they actually do. Users may believe that their chosen passwords are secure and cannot be easily guessed, even if they do not meet recommended complexity requirements (Zimmermann, Marky, & Renaud, 2022). The presence of these cognitive biases can result in the generation of passwords that are less strong than initially intended. After the user creates a suitable password for a particular account or system, the password enters its second lifecycle stage, maintenance. The user chooses how to remember the freshly generated password, for example, by memorising or storing using a method; to reduce memory interferences later on, he or she must also choose the ideal way to arrange, either physically or mentally, the freshly formed password with other active and current passwords (Choong, 2014). The Department of Defense's password policies, include memorising them, using them for just a year, not writing them down, and assigning them randomly. It follows that the fact that this information does not always equate to secure password management is not shocking (Tam, Glassman, & Vandenwauver, 2009). To ensure that the password has been correctly encoded into the long-term memory, the user must apply certain techniques (such as a mnemonic device, rote rehearsing, or typing the password several times to build muscle memory). Authentication, the final stage of the lifecycle, involves using the password to access the related account or system. Since the password will be used

repeatedly during its lifetime until a change event takes place, such as forgetting, having your password expire, having your password hacked, or wanting to synchronise your passwords across numerous accounts, the authentication stage is repetitive (Choong, 2014). It is necessary to authenticate using a username and password before retrieving credentials because these remote servers handle passwords for numerous users. On the other hand, because a user's mobile device is personal, portable managers never need a username (Karole, Saxena, & Christin). When a user exits the authentication stage and begins the subsequent password management lifecycle, their authentication experience whether favorable or negative may impact on how they generate new passwords. The research aims to analyse and comprehend the various factors contributing to human vulnerabilities in user password asset management. By conducting questionnaires to explore behavioral patterns, aim to shed light on the root causes of password-related security breaches and explore possible solutions to mitigate these risks effectively. By investigating these aspects, the study seeks to answer several key questions: What are the current password creation practices used by IT employees? How does user behavior impact these practices? Additionally, the research will explore whether implementing alternative authentication methods can effectively mitigate human-related cybersecurity risks within organisations.

2. Methodology

This chapter outlines the methodology used in this study, detailing the steps and techniques used for data collection. The methodology comprehends research and provides the framework for planning, design and development, and data collection and analysis. The study's population was selected based on research suitability, and a sampling procedure was used to choose specific samples. A pilot study was conducted to ensure accuracy before the main research. A data collection procedure was followed to document the entire process. A thorough research methodology is essential for understanding the vulnerabilities associated with human password practices. Descriptive analysis is employed as a key methodology, allowing for the exploration of complex password-related data and the extraction of meaningful insights. This approach enables the examination of patterns and trends in password management, including password change frequency, the prevalence of weak or easily guessable passwords, and patterns of password reuse. Additionally, the study will investigate psychological factors influencing user behaviour, such as cognitive biases and memory limitations.

i. Research Design

The research design involves three key stages: planning, designing and developing the research approach, and analysing the data to meet the study's deliverables and objectives. The survey method was used to gather data.

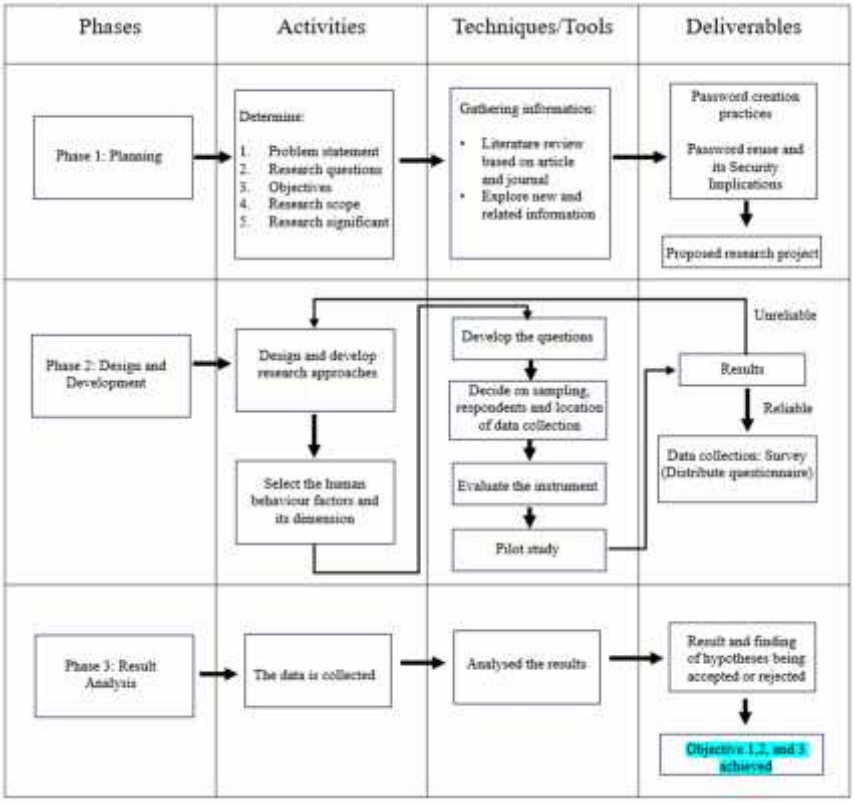

Figure 3: Full phases of research activities

ii. Phase 1: Planning

The planning phase involves developing a high-level strategy by defining the research problem, goals, scope, and significance. During this phase, the project was framed by reviewing existing literature on passwords, password creation, security, human behaviour, and related topics using sources such as Google Scholar and UUM eResources. The problem statements, research questions, objectives, scope, and significance were detailed in Chapter 1 based on this information.

iii. Phase 2: Design and Development

The design and development phase follows planning and involves applying descriptive analysis to extract meaningful insights from password-related data. This stage includes selecting research methods, survey participants, and materials. Specific actions and details for this phase are provided in the subsection below. A close-ended questionnaire was chosen as the primary data collection instrument. The questions were adapted from three related studies to address human vulnerabilities in password management. According to Narayanaswamy and Harinarayana, Google Forms is a suggested data management tool for creating online surveys (N. S. Narayanaswamy, 2016). The questionnaire was reviewed to ensure relevance to the research objectives. It consists of four sections: the first section gathers demographic information, while the remaining sections focus on password management vulnerabilities. All responses are confidential and used solely for research purposes. The prepared questionnaires adapted from previous research done by (Campbell, 2006), (Riley, 2006) and (Sporild, 2007). Additionally, a 5-point Likert scale, detailed in Table 3.1, was used to collect feedback from employees in the information technology department. The demographic questions, include queries about age, gender, role in the organisation, education level, and experience in the information technology field. For current password management practices, the questionnaire addresses how frequently participants change passwords, reuse them, share them in plaintext, use the same password for both organisational and personal accounts, and use password managers. These questions were adapted from (Campbell, 2006). The user behaviour section includes questions on the use of dictionary words in passwords, the inclusion of personal details, complexity of passwords (such as special characters), combinations of uppercase and lowercase letters, and repeated characters, with questions adapted from (Riley, 2006). The alternative authentication methods section, adapted from (Sporild, 2007), asks about exposure to various authentication methods, their perceived effectiveness compared to traditional passwords, success rates of these methods, their convenience, and personal preference for their use. Table 3.1 illustrates the 5-point Likert scale used to collect responses, ranging from "Never" to "Always." The online questionnaires were created using Google Forms. Prior to distributing the questionnaires to participants, a pilot test was conducted to ensure that the questions effectively gathered the required information and to identify any issues with wording or clarity. A pilot test serves as a preliminary experiment to assess the reliability of the questions and refine them as needed (N. S. Narayanaswamy, 2016). If the results from the pilot test were unreliable, further analysis was performed to address any uncertainties, and the questions were revised accordingly. Once the questionnaire was confirmed to be accurate, data collection commenced. The study was conducted at an Information Technology company in Singapore, focusing on a single project team. The sample size was determined based on research supporting the consistency of the sample, which reflects how well the sample represents the study population (Burmeister, Burmeister Nurse Researcher, & Aitken RN, 2012). A census approach was employed to include the entire team as the sample, thereby eliminating sampling error (Israel, 1992) The final data was collected from 134 participants, ensuring comprehensive coverage of the research population.

Table 1: The 5-point likert-scale

Never	Rarely	Sometimes	Often	Always

The data collection and analysis process will be managed digitally to enhance efficiency. The questionnaires are designed to be objective and standard. The use of questionnaire provides the interaction to be presented numerically. Prior to data collection, permission must be obtained from the organisation. The employees will be informed about the research objectives and their role as respondents. This clarification is essential to ensure that participants are willing and informed about their involvement. Respondents have the right to withdraw from the study at any time, and all data collected will be used solely for research purposes, kept confidential, and anonymised. The questions are crafted to be relevant and valid, applicable to a broad audience to support the research's goals.

iv. Phase 3: Data Collection and Analysis

The final phase of the study involves data collection and analysis. This stage focuses on understanding human vulnerabilities in password management by systematically examining related data. The goal is to identify weaknesses

and challenges in password practices, enabling individuals and organisations to improve their security measures. Descriptive analysis is used to uncover patterns, trends, and common issues in password management. This methodology involves gathering, measuring, classifying, computing, and interpreting quantitative data. Data analysis will involve frequency and percentage distributions, with results presented through charts and graphs for clarity. The aim is to provide a detailed view of current password practices, including how often passwords are changed, the prevalence of weak passwords, and other relevant behaviours. This analysis will also consider the psychological factors affecting password management, such as cognitive biases and memory constraints. The findings from this descriptive analysis will offer valuable insights into user behaviours and vulnerabilities, informing the development of targeted educational initiatives and improved security systems. By understanding common pitfalls and areas of vulnerability, the study aims to enhance password security practices and contribute to a safer digital environment. Descriptive statistics will summarise and outline participants' responses and characteristics related to password management (Nag & Ahmad Malik, 2023).

3. Results and discussion

To achieve a thorough understanding of the subject, this study included a comprehensive sample representing the entire population. By using the full population as the sample, the study eliminates sampling error and enhances the accuracy of the results. An in-depth analysis of the respondents' backgrounds is crucial for evaluating the data effectively and drawing meaningful conclusions. Current password management practices show varied frequencies of behaviour among users. Regarding the frequency of password changes, 0% never change their passwords, 16.4% rarely change them, 11.2% sometimes change them, 44.8% often change them, and 27.6% always change their passwords. In terms of password reuse, 17.9% never reuse passwords, 16.4% rarely do, 5.2% sometimes do, 32.1% often do, and 28.4% always reuse passwords. Password sharing occurs with 21.6% never sharing, 17.9% rarely sharing, 4.5% sometimes sharing, 32.8% often sharing, and 23.1% always sharing passwords. When it comes to using the same password for both organisational and personal accounts, 21.6% never do, 15.7% rarely do, 2.2% sometimes do, 36.6% often do, and 23.9% always do. As for storing passwords in a password manager, 15.7% never do, 21.6% rarely do, 3.7% sometimes do, 28.4% often do, and 30.6% always use a password manager. User behaviour also influences password creation practices. The use of dictionary passwords is distributed with 26.1% never using them, 18.7% rarely using them, 7.5% sometimes using them, 36.6% often using them, and 11.2% always using dictionary passwords. The incorporation of personal details in passwords happens with 21.6% never doing so, 20.9% rarely doing so, 6% sometimes doing so, 35.1% often doing so, and 16.4% always including personal details. Creating complex passwords shows that 13.4% never create complex passwords, 34.3% rarely do, 1.5% sometimes do, 28.4% often do, and 22.4% always create complex passwords. When creating passwords with a mix of uppercase and lowercase letters and numbers, 0% never do so, 13.4% rarely do, 6.7% sometimes do, 54.5% often do, and 25.4% always do. The use of repeated characters in passwords is seen with 30.6% never using them, 41% rarely using them, 4.5% sometimes using them, 17.2% often using them, and 6.7% always using repeated characters. Regarding the implementation of alternative authentication methods, exposure to different types of these methods is as follows: 0% never exposed, 9% rarely exposed, 6% sometimes exposed, 35.8% often exposed, and 49.3% always exposed. The perceived effectiveness of these methods is reported with 0% finding them never effective, 10.4% rarely effective, 7.5% sometimes effective, 44% often effective, and 38.1% always effective. The frequency of successful alternative authentication attempts is 0% never, 5.2% rarely, 11.9% sometimes, 46.3% often, and 36.6% always successful. As for the convenience of these methods, 9.7% find them never convenient, 38.1% rarely convenient, 7.5% sometimes convenient, 29.1% often convenient, and 15.7% always convenient. Finally, the preference for using alternative authentication methods for personal use is shown with 24.6% never preferring them, 36.6% rarely preferring them, 3.7% sometimes preferring them, 23.1% often preferring them, and 11.9% always preferring them.

Table 2: Summary of respondents' password practices, user behaviour, and implementation of alternative authentication method

Current password management practices	Never	Rarely	Sometimes	Often	Always
Frequency of password changes	0%	16.4%	11.2%	44.8%	27.6%

Frequency of password reuse	17.9%	16.4%	5.2%	32.1%	28.4%
Frequency of password sharing	21.6%	17.9%	4.5%	32.8%	23.1%
Frequency of using the same password for organisational and personal accounts	21.6%	15.7%	2.2%	36.6%	23.9%
Frequency of storing passwords in a password manager	15.7%	21.6%	3.7%	28.4%	30.6%
User behaviour influences password creation practices					
Usage of dictionary password	26.1%	18.7%	7.5%	36.6%	11.2%
Usage of personal details in password	21.6%	20.9%	6%	35.1%	16.4%
Creating passwords with complexity	13.4%	34.3%	1.5%	28.4%	22.4%
Creating passwords with a mix of uppercase, lowercase letters, and numbers	0%	13.4%	6.7%	54.5%	25.4%
Creating passwords with repeated characters	30.6%	41%	4.5%	17.2%	6.7%
Implementation of alternative authentication methods					
Exposure to different types of alternative authentication methods	0%	9%	6%	35.8%	49.3%

Effectiveness of alternative authentication methods	0%	10.4%	7.5%	44%	38.1%
Frequency of successful alternative authentication attempts	0%	5.2%	11.9%	46.3%	36.6%
Convenience of alternative authentication methods	9.7%	38.1%	7.5%	29.1%	15.7%
Preference to use alternative authentication methods for personal use	24.6%	36.6%	3.7%	23.1%	11.9%

Table 4.1 illustrates the summary of respondent's current password management practices, the influence of user behaviour on password creation practices, and the implementation of alternative authentication methods. Gaining insight into how individuals manage their passwords can reveal substantial insights into potential security vulnerabilities and cybersecurity awareness. The data shows that there are creditable behaviours among some users, but there are significant security vulnerabilities persist due to password reuse, password sharing in plaintext such as text files, emails, or other unencrypted methods, and using the same password for organisational accounts and personal accounts. The data reveals a range of user behaviour on password creation practices, from strong to weak. Dictionary words, personal information, and repetitive characters still pose a substantial risk even with the widespread understanding and adoption of complex passwords and mixed characters. Overall security can be improved by raising knowledge of and encouraging the use of strong password practices, such as avoiding personal information and dictionary words and regularly establishing complicated passwords. According to the research, there is an increasing number of users who are frequently or always exposed to alternative authentication methods and who find them to be successful and effective. Regarding their convenience, people have differing opinions; a sizeable portion of people find them infrequently or never convenient. Many users exhibit resistance to change and still favor traditional methods for personal usage, despite the efficacy and success rates of alternative authentication methods.

4. Conclusions

The user patterns for current password management practices are often changing the passwords. Anyhow, they practice reusing the password as it's easy and convenient to use and remembrance. This may occur because the policies are not strong enough to force the user to avoid reusing the passwords, at least for the last 5 recent passwords. This strict policy enforcement can force the user to avoid reusing passwords. They also practice sharing the passwords in plaintext or other unencrypted methods. This can be because they were not exposed to good encryption techniques. This may lead to high cybersecurity risks. The implementation of frequent audits in the application or the websites where they are using the passwords can improve the user password management practices. Moreover, users also highly use the same password for both organisational, which is work-related, and personal accounts. This could be a serious issue that needs urgent attention, as the user might be logging in to different social or any other third-party applications and websites since the developer or the system admins can access your passwords. They can misuse your passwords by blindly trying on any other platform. If the user uses the same passwords, the chances are high for compromising your other accounts. The user needs to separate their passwords. They must practice using different passwords for each and every account on the multiple platforms. So that they cannot be compromised easily and also can be traced back from which platform the data has been breached. If we use the same passwords on multiple platforms, it's hard to identify the sources of the data breach. The user often uses password managers. This seems to be a good password management practices, which everyone should adopt, as this can improve the chances of passwords being breached and improve the overall security posture. The analysis of user behaviour that influences the password creation practices for the use of passwords that are found in a standard dictionary or common word lists (e.g., "password123," "qwerty," or "letmein") is often. This clearly indicates that the

user is often exposed to commonly used passwords. This can lead to high chances for dictionary attacks. The attackers can compromise your accounts by using a pre-compiled list of common password words to guess the passwords. It will exploit the tendency for users to choose guessable passwords. Encourage the user to use passphrases or random combinations of words and characters. Provide examples of complex passwords that avoid common patterns. The user also creates passwords using personal details such as your name, birthday, or other easily identifiable information often. This may lead to identification theft. Attackers will target the user and will perform social engineering to gather all that personal information. Then they will try to guess the passwords using that information. To avoid that, users need to be educated on avoiding common pitfalls. Most the users rarely create passwords with complexity, such as including special characters. In an effort to simplify their lives, users might choose passwords that are easier to remember but less secure, prioritising convenience over security. Conduct regular training or awareness campaigns about the risks associated with weak passwords and the benefits of strong password practices. Use real-world examples and statistics to emphasise the importance. Increases user awareness and motivates them to adopt better password practices by understanding the potential consequences of weak passwords. The users often create passwords that include a combination of uppercase letters, lowercase letters, and numbers. This would be the best practice since the base guidelines for most of the platforms already make this mandatory. Moreover, the user also rarely creates passwords that contain the same character repeated three or more times (e.g., "aaabbb," "111111," "@@@@"). From this analysis, we can know that users are aware of the basic concept of good password creation practices. The users are always exposed to different types of alternative authentication methods. Alternative authentication methods are often considered more effective than traditional passwords in enhancing cybersecurity. This is because they can provide a higher level of security through something the user is (biometrics), has (a token), or knows (a password combined with another factor). They can protect against common threats password theft and brute-force attacks more effectively than passwords alone. The users believe that alternative authentication methods are effective in enhancing cybersecurity compared to traditional passwords, often. Users generally experience successful authentication with these methods because they are designed to be robust and less susceptible to common security issues. For instance, biometrics are difficult to replicate, and hardware tokens generate time-based codes that are hard for attackers to intercept and reuse. This results in a high success rate for authentication attempts when using these methods. Despite their effectiveness, users often find alternative authentication methods inconvenient for several reasons. Some methods, like setting up and using hardware tokens or MFA apps, can be more complex than simply typing a password. The process of authentication might be slower or involve additional steps compared to the straightforward act of entering a password. Due to the inconvenience, many users choose not to use alternative authentication methods for their personal accounts. They might find it easier to stick with traditional passwords, despite knowing that alternative methods are more secure. Personal accounts often don't seem as high-risk to many users compared to professional or sensitive accounts, leading to lower adoption of more secure methods for personal use. However, the users should be more concerned with security instead of convenience, as this has strong security authentication mechanisms and mitigates the cybersecurity risks. Users should prioritise the alternative authentication methods to practice using them for personal accounts. The implementation of alternative authentication methods effectively mitigates human-related cybersecurity risks in organisations. In conclusion, the examination of existing password practices indicates notable discrepancies that are impacted by user behaviour, underscoring the necessity of better policies and education to strengthen password security. The analysis highlights the crucial influence that user behaviour, has on these methods' efficacy and shows how important human factors are to the security landscape. Moreover, the assessment of substitute authentication techniques has demonstrated that these technologies can significantly reduce cybersecurity risks associated with human interaction. Emerging issues in cybersecurity will require a combination of improved password restrictions, user education, and sophisticated user-friendly authentication techniques.

Acknowledgments

The authors would like to thank Universiti Utara Malaysia.

References

Alnifie, K. M., & Kim, C. (2023, April). Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis. Journal of Information Security, 14(2), 93-110.

Alsharif, M., Mishra, S., & AlShehri, M. (2021, June 8). Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science & Engineering, 40(3), 1153-1166.

Burmeister, A., Burmeister Nurse Researcher, E. B., & Aitken RN, L. M. (2012, July 26). Sample size: How many is enough? Official journal of the Australian College of Critical Care Nurses Ltd, 25(4), P271-274.

Campbell, K. B. (2006, November). "User behaviours associated with password security and management.,". ustralasian Journal of Information Systems, vol. 14(no. 1), pp. 81-100.

Choong, Y. Y. (2014). A cognitive-behavioral framework of user password management lifecycle. In Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014 (pp. pp. 127-137). Heraklion, Crete, Greece: Springer International Publishing.

Eve, M. P. (2016). Password. Bloomsbury Academic.

Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., . . . Ome, U. (2023, May). Password-Based Authentication and The Experiences of End Users. Scientific African 21, e01743.

Gangwal, A., Singh, S., & Srivastava, A. (2023, April). AutoSpill: Credential Leakage from Mobile Password Managers. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy, 39-47.

(2022). IBM X-Force Threat Intelligence Index. IBM.

Israel, G. D. (1992). Determining sample size.

Karole, A., Saxena, N., & Christin, N. (n.d.). A comparative usability evaluation of traditional password managers. In Information Security and Cryptology-ICISC 2010: (pp. pp. 233-251). 13th International Conference, Seoul, Korea, December 1-3, 2010, Revised Selected Papers 13: Springer Berlin Heidelberg.

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

N. S. Narayanaswamy, V. R. (2016). "Online Survey Tools: A Case Study of Google Forms,".

Nag, M. B., & Ahmad Malik, F. (2023, January 2). Data analysis and interpretation. In Repatriation Management and Competency Transfer in a Culturally Dynamic World, 93-140.

Otta, S. P., Panda, S., Gupta, M., & Hota, C. (2023, April 10). A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. Future Internet, 15(4), 146.

(2023). Password Usage and Security Report. Dashlane.

Riley, S. (2006, February). "Password security: What users know and what they actually do.,". Usability News, vol. 8(no. 1), pp. 2833-2836.

Scarfone, K., & Souppaya, M. (2009). Guide to enterprise password management (draft). . NIST special publication, 38.

Sporild, M. (2007). "Method for evaluating authentication system quality,". Gjøvik: Faculty of Computer Science and Media Technology, Gjøvik University College.

Stobert, E., & Biddle, R. (2015). Expert password management. In Technology and Practice of Passwords. 9th International Conference, PASSWORDS 2015, (pp. pp. 3-20). Cambridge, UK: Springer International Publishing.

Tam, L., Glassman, M., & Vandenwauver, M. (2009, July 31). The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology, 29(3), 233–244. Retrieved from https://doi.org/10.1080/01449290903121386

The Importance of Password Security. (2024, April). Retrieved April 2024, from https://www.linkedin.com/posts/clyrofor_clyrofor-keepingitlocked-cybersecurity-activity-7179356692025860096-TA1U/

Ugwu, C., Ani, C., Ezema, M., Asogwa, C., Ome, U., Obayi, A., . . . Ukwandu, E. (2022, April). Towards Determining the Effect of Age and Educational Level on Cyber-Hygiene. In 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), 1-5.

Verizon. (2023). Data Breach Investigations Report (DBIR). Verizon.

Wang, Q., & Wang, D. (2022). Understanding failures in security proofs of multi-factor authentication for mobile devices. IEEE Transactions on Information Forensics and Security, 18, 597-612.

Zimmermann, V., Marky, K., & Renaud, K. (2022, March). Hybrid password meters for more secure passwords–a comprehensive study of password meters including nudges and password information. Behaviour & Information Technology, 42(6), 700-743.