I. J. Education and Management Engineering, **2024, 1, 33-40**
Published Online on February 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijeme.2024.01.04

Exploring Perceptions and Habits of Sri Lankan Users: A Study on Password Management and Adoption of Password Managers

Prageeth Fernando*
Faculty of Technology, University of Sri Jayewardenepura, Colombo, Sri Lanka
E-mail: prageethfndo@gmail.com
ORCID ID: https://orcid.org/0000-0001-7567-6863
*Corresponding author

Received: 02 July, 2023; Revised: 13 August, 2023; Accepted: 14 September, 2023; Published: 08 February, 2024

Abstract: This research paper investigates the attitudes and behaviors of Sri Lankan internet users toward passwords and password managers. The study addresses the security flaws and malpractices associated with passwords and aims to identify effective password management solutions. Two surveys were conducted, one focusing on user attitudes and strategies related to passwords, and the other evaluating user experiences with decentralized offline password managers. The findings reveal that a significant portion of the participants employed complex password-creation strategies and utilized various methods for storing and reusing passwords. Male participants and individuals in the 20-29 age group were predominant in the study. Surprisingly, only a minority of participants had received training in password creation and management. The analysis also indicated that participants without training tended to create easily breakable passwords, while those with training opted for more complex and stronger passwords. In terms of password management methods, participants without training relied on manual note-taking or memorization, while those with training preferred secure password managers. Furthermore, the study found a higher prevalence of password reuse among participants who used manual password creation methods compared to those who used password generators. The research underscores the need for improved password management practices and increased awareness among Sri Lankan internet users. The findings introduce novel insights into the existing knowledge of password management and lay the groundwork for developing targeted interventions and strategies to enhance security in the Sri Lankan online landscape.

Index Terms: Passwords, Password literacy, Password managers, Malpractices

1. Introduction

Ever since the Massachusetts Institute of Technology (MIT) created the Compatible Time Sharing System (CTTS), the first computer system with a password login implementation in 1961, passwords have become the primary method of controlling and authenticating access to any computer information system [1]. Notwithstanding the well-known security flaws, passwords remain the standard method of authentication for nearly all online services. Passwords accomplish extremely poor performances in terms of security, as studies have repeatedly proven. Worse, there is an increasing trend of users registering for an increasing number of online services. Because of the increasing number of required passwords, as well as the limited human capacity to remember passwords, the bad practice of reusing passwords across accounts has emerged.

To address the situation, users are frequently directed to password managers as a solution to the problems of password reuse and vulnerabilities. Nevertheless, the actual impact of password managers on both online accounts and user security has not been thoroughly studied to date. This study aims to address this critical gap by investigating the role and effectiveness of password managers in enhancing online security within the Sri Lankan context. With the rapid development and implementation of IT throughout Sri Lanka, security has become very important while its significance remains hidden and silent [2]. In Sri Lanka, there are approximately 11.34 million internet users out of a population of 21.5 million people, with 52.6 percent penetration and a 4.9 percent increase from 2021 to 2022 [3]. Specifically, by assessing existing solutions, their strengths, limitations, and their impact on user security. By doing so, valuable insights and recommendations are sought to be provided for the improvement of user security practices in Sri Lanka's evolving online landscape.

2. Related Work

Studies on the topic of "Perception and Habitual Attitudes of Sri Lankan People Towards Computer Passwords and Password Managers" are more limited than studies done based on the global phenomenon. Several studies [4, 5,6,7,8,9,10] have provided crucial context on people's habits and attitudes toward password management. A recent study [11] indicates that the average user holds 16 to 26 password-protected online accounts actively and users habitually struggle to memorize the passwords, especially password that has to be created or randomly generated under certain requirement of a website or a system that is in infrequent usage. The number of passwords to remember is increasing in tandem with the number of accounts per user. This puts a noticeable strain on human memory, which users try to compensate for by writing them down, reusing them, or choosing overly simple and easily breakable passwords [12].

Some studies [4,7,8,11] discuss various factors that affect user perception and techniques for managing passwords efficiently, while several [5,13,14] have proposed new authentication mechanisms to replace typical password authentication with biometric authentication, OTP/PIN codes, security tokens, and authentication apps. The majority of the studies that propose alternative mechanisms recommend biometric authentication since it addresses all the recognized issues of passwords and password management [13].

Among the studies that have been done on password management, [6,12,15] studies have discussed the factors of password creation, reuse, sharing, and strength in contrast to forced password memorization. Woods and Siponen [7] have evaluated user password memorability by password re-verification three times can increase memorability by up to 20% compared to current practices. But it also clearly discusses that forced memorability improvement leads to low user convenience and incautious behaviors towards the system. Kankane, DiRusso, and Buckley [10] studied the effectiveness of password management based on 5 types of nudges that can be enforced on users for better password management. In the study measures, they stated that the latter finding is not likely to be in favor of the initially expected outcome. Nudges are not effective enough to produce behavioral change among users but are effective in fashion for influencing attitude change. None of the nudges has any significant effect on password creation though salience influenced a level of comfort in keeping generated passwords.

According to the findings of the study [8], before organizations implement password policy guidelines, they must first determine their users' attitudes toward such guidelines. It was discovered that certain human factors such as human memory, attitude, and apathy frequently cause users to adopt insecure coping strategies such as reusing passwords, writing down passwords, and not changing passwords. Habib et al., [9] also argue that enforcing password policies has only little impact on user behaviors and attitudes. Enforced password policies lead the users to predictable password updates and are exposed to an increased vulnerability rate than before.

Some studies indicate the utilization of password managers for more efficient password management among computer users [4,11,14]. Password generation utilizing password managers is more productive in contrast to manual creation in consideration of factors such as password length, strength reuse, and update. However, Pearman et al. [11] argue that password managers suffer from a low acceptance rate among regular online account holders due to potential security vulnerabilities. They also argue that users tend to utilize web browser-based password managing to autofill passwords. Their study reveals that unencrypted password data could be found in temporary files and risk attackers gain to physical devices or web browsers and pose a threat to the user identity and security. These web browser-based password managers are also encouraging users to reuse passwords since no password reuse avoidance or mitigation mechanism is implemented in default. Anand and Balakrishnan [13] state that users' retraction from password managers is because of third-party data handling. According to this study, users are concerned about the cloud storage of their sensitive data and passwords. Therefore, they studied on SESS algorithm to ensure security and privacy in various cloud service providers. Their expected result was significantly varied from the actual outcome of the study and decreased efficiency is shown in the study than the efficiency shown by the password manager utilization.

3. Proposed Methods

Understanding user perception & habitual attitudes towards passwords and password managers was accomplished by designing two separate surveys and distributing them in both offline (paper-based) and online (Google Forms) modes. The first survey is more focused on how users perceive passwords, user habitual attitudes towards passwords, and how users interact with password protections. The second survey is more concentrated on determining user experience with decentralized offline password managers over popular centralized cloud-based password managers.

3.1 Data Collection

Both surveys were conducted by randomly selecting participants from all 25 districts in Sri Lanka and delivering primarily in English with assistance from Sinhala and Tamil when needed. Purposive sampling was used to ensure that interviewed participants who used a variety of password-management strategies, such as non-technological approaches (e.g.: - writing passwords in a notebook), computer-based approaches that did not involve specific password management software (e.g.:- saving passwords in an Excel spreadsheet), password managers built into operating systems (e.g.:- Apple Keychain), web browser based password management (e.g.:- Chrome auto-fill), and separately installed password managers. When the sample included diversity in terms of age, profession, and technical proficiency of participants from each of the above categories, response acceptance was stopped. Lastly, 200 & 30 participants and 26 & 10 survey questions were interviewed from participants for the first and second surveys respectively.

The first questionnaire was designed to examine users about their perceptions and habitual attitudes toward passwords and their management. The questionnaire consists of a total of 26 questions including 21 multiple-choice single-answer questions, 3 multiple-choice multi-answer questions, 1 dropdown question, and 1 short-answer question. This questionnaire contained general and specific questions about computer security background, password creation, reuse, sharing, memorization, strength, and management. Participants were questioned about their general attitudes toward privacy, their habitual attitudes toward passwords, their skills, and strategies for creating and managing passwords, as well as fundamental demographic and online safety questions. On one hand, this information allows us to get a general overview of common password creation and storage strategies. On the other hand, this information assists in detecting and avoiding potential biases in the later stages of this research study.

The second survey was conducted to evaluate the level of user experience with the decentralized offline password managers. For this survey, both categories of users with prior experience with password managers and users with no prior experience with password managers participated in balanced quantities. The questionnaire consists of a total of 10 questions including 7 multiple choice questions, 2 linear scale questions, and 1 short answer question. This questionnaire is more concentrated on evaluating the decentralized offline password managers' user experience compared to memorizing, popular centralized cloud-based password managers, and other methods. The second questionnaire thoroughly evaluates user responses on the major factors such as offline local storage of user credentials, distrusted architecture, random password generation, secure backup, and encryption on decentralized offline password managers. Participants were questioned about their past and present use of password managers, with their opinion on above mentioned factors.

3.2 Data Analysis

3.2.1 Data Preprocessing

Preparing the dataset for analysis involves data preprocessing. Data cleansing, dimensionality reduction, and handling missing and null values are a few of the activities that make up this process. Preprocessing was done using Weka tools on the data obtained from the two questionnaires. The available data was first organized, sorted, and combined for both survey responses.

3.2.2 Visual analysis

To understand correlations, all attribute data were visualized after preprocessing. In applied behavior analysis research, the descriptive technique of visual analysis (VA) is frequently employed. An AB model, which examines the target behavior both before and after the intervention, is the most fundamental experimental model used in single-case designs. The VA conducted by a judge or rater is based on a set of standards that assess and contrast phase A and phase B characteristics and determine whether behavior changes seen in phase B are a result of the intervention. Visual analyses are focused on the understanding correlation between 'Preferred passwords against password creation training background', 'Preferred password management method against password management training background', and 'Password reuse frequency against password creation method'.

3.2.3 Naïve Bayes Classifier

Based on the result set of the first questionnaire, the Naïve Bayes algorithm was used to predict the correlations between user perception attributes and password management attributes. The Naïve Bayes classifier is a classification model that is based on the Bayes theorem which predicts the effect of one attribute is independent of other attributes. Feature extraction was done to identify critical attributes that have effects on password management method utilization.

3.2.4 J48 Decision Tree

Then, to categorize the attributes that create the connectivity of correlation nodes, the J48 tree classification method was used. J48 employs a top-down strategy of recursive divide and conquer. At the root node, you choose which attribute to split on, and then you create a branch for each possible attribute value, which splits the instances into subsets, one for each branch that extends from the root node. The same methodology was used for an analysis of 'avoidance characteristics' of popular centralized cloud-based password managers against preferred characteristics of decentralized offline password managers based on second survey responses.

4. Results

4.1 Survey 1

The majority of the interviewed participants had complex password creation strategies and different storing & reusing methods. A total of 200 participants responded to the first survey.

Table 1. Survey 1 Demographic Results

Demographics		
Gender	Number of responses	%
Male	117	58.5
Female	83	41.5
Age	Number of responses	%
10-19	31	15.7
20-29	88	44.1
30-39	47	23.6
40-49	24	11.8
50-59	10	4.7

Table 2. Computer security background

Computer security training background		
Training on computer security		
Yes	94	46.8%
No	106	53.2%
Training on password creation/generation		
Yes	84	42.1%
No	116	57.9%
Training on password management		
Yes	73	36.2%
No	127	63.8%

As shown in Table 1, the majority of respondents (58.5%) were male, while 41.5 percent were female. The 20-29 age group had the highest total of respondents (44.1%), followed by the 30-39 age group (23.6%). According to Table 2, only 36.2 percent of the 200 participants have prior experience with password management training, while 94 have a background in computer security training. 57.9 percent (116) of those who responded had no prior experience creating or generating passwords.

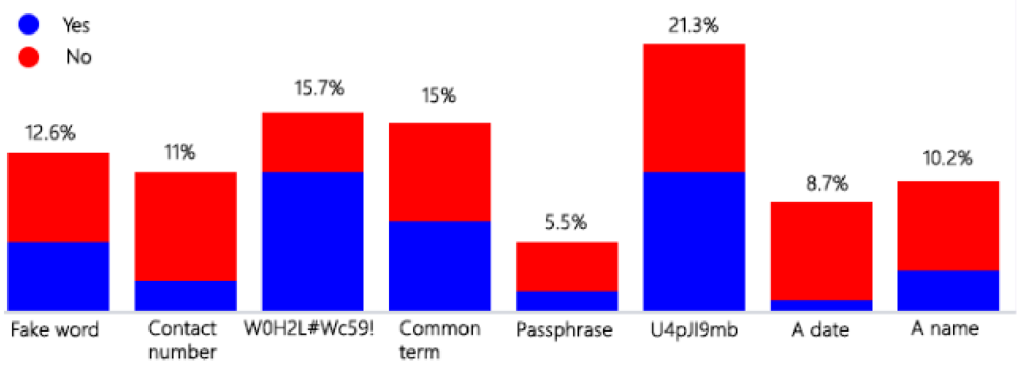

Fig.1. Preferred passwords against password creation training background

Fig.1 presents different password types that respondents selected for a permanent online account against their password creation training background. According to the results of the 'preferred passwords against password creation training background' analysis, the majority of respondents who do not have any password training background on password creation or generation (69.7%) tended to create passwords based on names, dates, passphrases, and contact numbers which are easily breakable and possess security threats to their online accounts or digital security while the majority of respondents who have password training background on password creation or generation (70.8%) has chosen more complex and strong passwords. Stobert and Biddle [6] have discussed the correlation that exists between password literacy and password management, and this analysis proves that the introduced correlation is valid for the Sri Lankan user context as well.

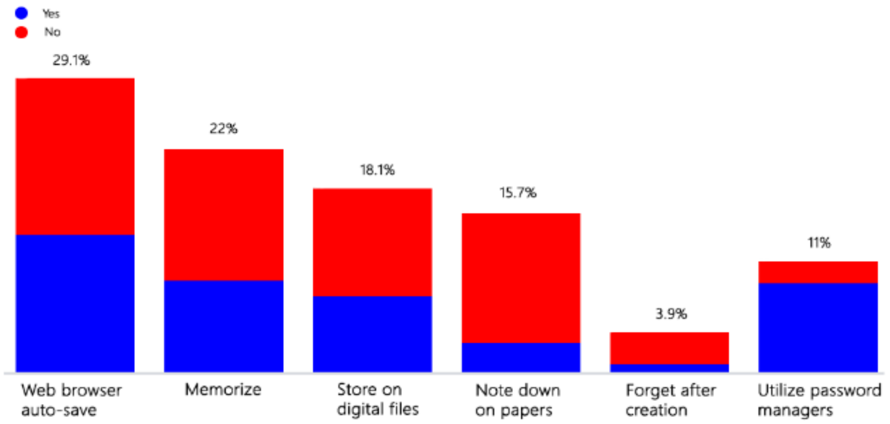

Fig.2. Preferred password management method against password management training background

Fig.2 presents different password storing or management methods that respondents selected for their online accounts against their password management training background. According to the results of the 'preferred password management methods against password management training background' analysis, the majority of respondents who do not have any training background in password management tended to note down their passwords on paper manually or to memorize them. Respondents who selected 'Forget after creation' (3.9%) stated that they had no reason to be concerned about the security of their accounts.

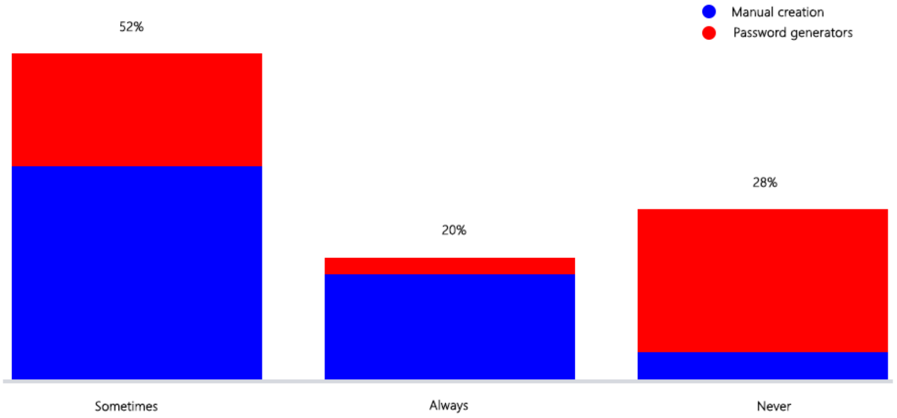

Fig.3. Password reuse frequency against password creation method

Fig.3 presents the analysis results of the password reusing frequency of respondents against manual password creation and password generator utilization. According to Fig.3, respondents who utilize password generators (38.4%) for their password creation are more tend to lower their password reuse and create different passwords. Furthermore, respondents who utilize manual password creation tend to increase their password reuse frequency. Particularly, those respondents who manually create passwords tend to generate new passwords that are only minor modifications of their existing passwords.

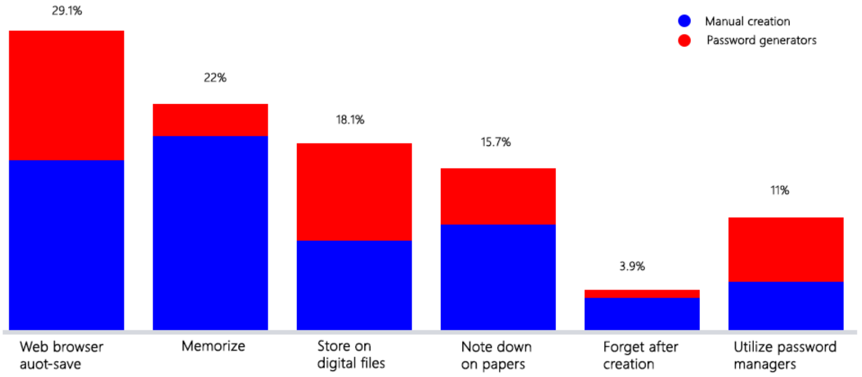

Fig.4. Preferred password management method against password creation method

Fig.4 presents the analysis results of different password storing or management methods that respondents selected for their online accounts against manual password creation and password generator utilization. The majority of the respondents (61.6%) are biased toward manual password creation rather than password generator utilization. The respondents who utilize password generators are more tended to store and manage their passwords on web browsers, password manager software, and digital files. Memorizing is at a significantly lower rate among these respondents because of the complexity of generated passwords. The majority of manual creation respondents are utilizing memorization, web browser auto-save, and paper note-down methods while 3.2 percent forget passwords after creation.

4.2 Survey 2

The majority of the second survey respondents (73.4%) have used the decentralized offline password managers and among the respondents, 62.8 percent have prior experience with various password managers. According to respondents, password managers are more effective than memorizing passwords in 73.9 percent of cases, and decentralized offline password managers are superior to other password management strategies in 60.9 percent of cases.

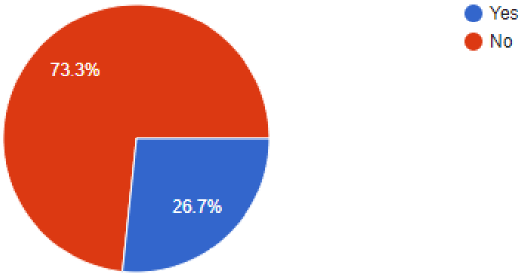

Fig. 5. Preference for moving into the cloud-based password managers

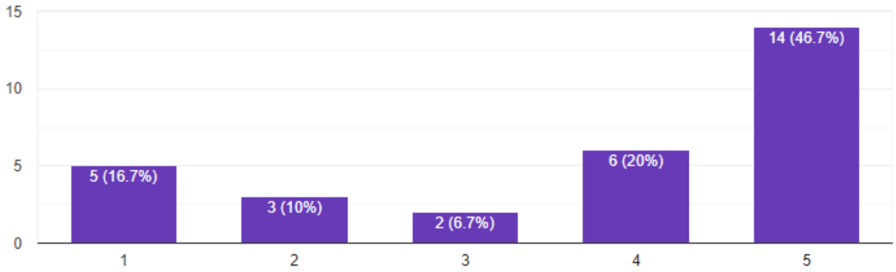

Fig. 6. Ratings on “offline local storage of user credentials”

Fig.5 and Fig.6 present respondents’ preference for moving into the cloud and respondents’ ratings on the ‘offline local storage of user credentials’ feature respectively. According to the analysis 73.3 percent, of respondents are at odds with storing passwords on third-party storage on the cloud and entertained with the ‘offline local storage of user credentials’ feature. According to survey responses, the decentralized offline password managers received a 3.8 rating out of 5.

5. Discussions

This study’s findings highlight tradeoffs between Sri Lankans' security concerns over password management and their adoption of password managers. As with password creation, various factors can influence password reuse. In general, survey respondents exhibited very similar password strength and reuse characteristics to those observed in previous studies, and this study may reaffirm prior findings while also demonstrating that the generation mechanism is a major factor that has a significant effect on creation strength and reuse frequency. Furthermore, survey findings on password reusing are fair to the findings of Lyastani et al. [12], indicating that the creation of a new password is frequently a minor variation from an old password. Extending further, this study could establish a correlation between manual password creation and the frequency of password reuse.

Survey result analysis done on management training background against password management methods [Fig.2] implies a significant reluctant of password manager utilization among the users because most of the password managers available in the market are cloud-based and people hesitate to put sensitive data like passwords and other online account credentials on a third-party hand. This privacy concern of the users cannot be neglected. Therefore, 59.1 percent of literate people practice memorization, digital file storing, or web browser auto-save. Memorization is considered the best password management mechanism but with the increasing number of online accounts, it is an impractical method [15]. Though 34.6 percent of literate respondents utilize web browser auto-save, it is not recommended due to its built-in security flaws such as unencrypted password data that can be found on temporary files, and inefficiencies but because of lack of options.

Analyses on ‘Password reuse frequency against password creation method’ and ‘Preferred password management method against password creation method’ imply when users try to create complex passwords by manual creation and eliminate or reduce password reuse frequency, they will be led to unsecured password management methods. 58.7 percent of respondents stated that noting down on paper and storing on digital files as their conventions to manage when they are forced to create policy-enforced complex passwords. Education, computer literacy, password management training, priorities, and privacy concerns can be identified as factors from the experimented study, in addition to the factors that determine the amount of effort a user is willing to put into creating stronger passwords presented in several studies [4,6,11].

The result analysis of the second survey declares that distributed local password managers are more at ease with their privacy policy because of its all-in offline local availability and the distributed feature where the user has full control over all data and passwords stored in the application. As discussed in some studies [6,13], centralized cloud-based password managers grant distinct advantages to their users such as convenient auto-filling, cross-platform availability, and secure password sharing. These special features enabled password managers can only be supported if the cloud-based convention is followed but along with the discussion so far in this paper, it is clear that the majority of the literate users are not entertaining third-party sensitive and password data handling. Although as identified by Fredericks [8], the limitation of human factors leads users to password manager adoption, people who have password literacy do not tend to risk their privacy on this coping strategy. One of the most serious security flaws of password managers is that if the master password is compromised, an attacker or hacker can steal all of a user's stored passwords and other sensitive data. This single point of failure discourages the user from utilizing password managers.

One of the major limitations of the study is the majority of the participants are from the age group of 20-29 and they might not reflect the Sri Lankan general population’s perception and attitude towards passwords and password management. Another major limitation was the language barrier since the first survey was responded to by participants scattered all over the island with different levels of education. Due to the research area’s sensitivity, a lot of participants tended to skip the survey or self-report inaccurate data to protect their privacy and safety. Additionally, the study utilizes self-reported data from participants’ past behaviors which might have been forgotten or reported incorrectly. Using password managers is not regarded as an unsafe coping strategy. However, there is no mention of password managers in any of the standards or best practices. One method of addressing the human factors associated with password management is through education, training, and awareness.

6. Conclusions

This empirical study examined user perception and habitual attitudes of Sri Lankan people toward computer passwords and password managers. Two surveys were designed and distributed using paper forms (physical) and Google Forms (online). The first questionnaire included 26 general and specific questions about computer security background, password creation, reuse, sharing, memorization, strength, and management. The second questionnaire included 10 questions about user experience in dealing with password management and memorization problems. The results show that most of the respondents showed a lack of knowledge and training for dealing with computer passwords and their management which is due to several influential factors such as education, computer literacy, amount of effort, priorities, and privacy concerns. The first survey findings indicate that users who are aware of password managers are reluctant because of third-party password management and cloud storage of passwords. The majority of the respondents were uncomfortable with third-party password handling. In addition, the second survey provided evidence for this by presenting the majority towards keeping away from a cloud environment. People who care more about password managing privacy are deemed to be satisfied with the offline local storage of user credentials. We may envision various alleyways for future work through this study. One potential direction is to explore the integration of diverse and innovative password generators into management practices. Furthermore, this approach can be used to investigate password managers' influence in various ecosystems to facilitate cross-platform availability.

References

[1] R. Morris and K. Thompson, “Password security: a case history,” *Commun. ACM*, vol. 22, no. 11, pp. 594–597, 1979, doi: 10.1145/359168.359172.

[2] R. Nagahawatta, M. Warren, and W. Yeoh, “A Study of Cybersecurity Awareness in Sri Lanka A Study of Cybersecurity Awareness in Sri Lanka,” 2020.

[3] S. Kemp, “Digital 2022: Sri Lanka,” *DataReportal – Global Digital Insights*, 2022. https://datareportal.com/reports/digital-2022-sri-lanka

[4] R. Macgregor, “USER COMPREHENSION OF PASSWORD REUSE RISKS AND MITIGATIONS IN PASSWORD MANAGERS,” 2020. Accessed: Jan. 01, 2023. [Online]. Available: https://dalspace.library.dal.ca/bitstream/handle/10222/78416/MacGregor-Robbie-MCSc-CSCI-April-2020.pdf?sequence=1

[5] M. Lennartsson, “Evaluating the Memorability of Different Password Creation Strategies: A Systematic Literature Review,” 2019.

[6] E. Stobert and R. Biddle, “The Password Life Cycle,” *ACM Trans. Priv. Secur.*, vol. 21, no. 3, pp. 1–32, 2018, doi: 10.1145/3183341.

[7] N. Woods and M. Siponen, “Improving password memorability, while not inconveniencing the user,” *Int. J. Hum.-Comput. Stud.*, vol. 128, pp. 61–71, 2019, doi: 10.1016/j.ijhcs.2019.02.003.

[8] D. Fredericks, “Users’ Perceptions Regarding Password Policies,” 2018.

[9] H. Habib *et al.*, “Open access to the Proceedings of the Fourteenth Symposium on Usable Privacy and Security is sponsored by USENIX. User Behaviors and Attitudes Under Password Expiration Policies User Behaviors and Attitudes Under Password Expiration Policies,” 2018.

[10] S. Kankane, C. DiRusso, and C. Buckley, “Can We Nudge Users Toward Better Password Management?,” *Ext. Abstr. 2018 CHI Conf. Hum. Factors Comput. Syst.*, 2018, doi: 10.1145/3170427.3188689.

[11] S. Pearman, S. Zhang, L. Bauer, N. Christin, and L. Cranor, “Open access to the Proceedings of the Fifteenth Symposium on Usable Privacy and Security is sponsored by USENIX. Why people (don’t) use password managers effectively Why people (don’t) use password managers effectively,” 2019.

[12] S. Lyastani, M. Schilling, S. Fahl, M. Backes, and S. Bugiel, “Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse,” 2018.

[13] S. Anand and S. Balakrishnan, “Challenges and issues in ensuring safe cloud based password management to enhance security,” 2019.

[14] M. Abuzaraida and A. Zeki, “Collection of Handwritten text View project Development of Malay Online Virtual Integrated Corpus (MOVIC) for Sentiment Analysis using Web-scraping View project AWARENESS AND SECURITY ISSUES IN PASSWORD MANAGEMENT AMONG LIBYAN UNIVERSITIES STAFF MEMBERS,” *Artic. ID IJARET1112123 Int. J. Adv. Res. Eng. Technol.*, vol. 11, no. 12, pp. 1292–1303, 2020, doi: 10.34218/IJARET.11.12.2020.123.

[15] E. Kuka and R. Bahiti, “Information Security Management: Password Security Issues,” *Acad. J. Interdiscip. Stud.*, vol. 7, no. 2, pp. 43–47, 2018, doi: 10.2478/ajis-2018-0045.

Author’ s Profile

Prageeth Fernando is a graduate from the University of Sri Jayewardenepura, having earned a Bachelor of Information and Communication Technology with First-Class Honours in 2023. With a specialization in Network Technology, he has made significant strides in the field, demonstrated by authoring five journal articles and holding the roles of System Administrator and IT Support Engineer. As a skilled Project Manager, he has successfully overseen eight projects. Notably, his research interest centers on the innovative concept of replacing the human factor within the security chain, reflecting a commitment to advancing the frontiers of cybersecurity.

How to cite this paper: Prageeth Fernando, "Exploring Perceptions and Habits of Sri Lankan Users: A Study on Password Management and Adoption of Password Managers", International Journal of Education and Management Engineering (IJEME), Vol.14, No.1, pp. 33-40, 2024. DOI:10.5815/ijeme.2024.01.04