future internet

MDPI

Article

Password Managers—It's All about Trust and Transparency

Fahad Alodhyani *, George Theodorakopoulos and Philipp Reinecke

School of Computer Science and Informatics, Cardiff University, Queens Building, Cardiff CF24 3AA, UK; theodorakopoulosg@cardiff.ac.uk (G.T.); reineckep@cardiff.ac.uk (P.R.)

* Correspondence: alodhyanifs@cardiff.ac.uk

§ This PDF version contains corrections to the publisher's version.

Received: 28 September 2020; Accepted: 27 October 2020; Published: 30 October 2020

Abstract: A password is considered to be the first line of defence in protecting online accounts, but there are problems when people handle their own passwords, for example, password reuse and difficult to memorize. Password managers appear to be a promising solution to help people handle their passwords. However, there is low adoption of password managers, even though they are widely available, and there are fewer studies on users of password managers. Therefore, the issues that cause people not to use password managers must be investigated and, more generally, what users think about them and the user interfaces of password managers. In this paper, we report three studies that we conducted: on user interfaces and the functions of three password managers; a usability test and an interview study; and an online questionnaire study about users and non-users of password managers, which also compares experts and non-experts regarding their use (or non-use) of password managers. Our findings show that usability is not a major problem, rather lack of trust and transparency are the main reasons for the low adoption of password managers. Users of password managers have trust and security concerns, while there are a few issues with the user interfaces and functions of password managers.

Keywords: password manager; human factor; security; usability; trust; transparency; user interface

1. Introduction

Passwords continue to be used for authentication in spite of consensus by researchers that we need to have something more user-friendly and secure [1]. A password is considered the most popular method of authentication due to its cost-effectiveness and simplicity [2]. However, people create weak and short passwords, reuse the same password for multiple accounts, write them down and include personal information. Because of human memory limitations, users find it difficult to memorise strong, long and random passwords that are hard to crack [3]. Li et al. analysed a leaked password data set from a Chinese website and found that passwords contain personal information such as names and dates of birth [4]. Thousands of passwords have been compromised in the last few years because of using personal information in passwords, writing passwords down and reusing the same password for multiple accounts.

In response to these problems, a number of tools have been developed to help people handle their passwords, such as random password generators and password managers. Florêncio et al. state that if a password manager is not used, grouping accounts and reusing passwords become the only manageable solution [5]. So, organizations should consider providing password managers with a built-in generator because people might not create and preserve passwords themselves [6]. In fact, a password manager may be a suitable solution to help people store and manage their own passwords and generate a unique password for each account.

Ion et al. state that the low adoption rate for password managers by people might be due to a lack of understanding of the security benefits of these tools [7], because people view them as a security risk [8,9] or, because of usability drawbacks [9,10], a lack of trust [11]. So, there is no obvious reason why people do not use password managers even though they are widely available. Existing literature mainly focuses on passwords, but rarely on password managers; therefore, there is no clear answer to the question of low adoption. More to the point, previous work has rarely focused on users of password managers and their perspective. Thus, it is possible that users have similar issues as non-users in terms of trust, security and transparency. Also, to the best of our knowledge, no study has evaluated the user interfaces of password managers, which may be a reason that discourages non-users from using them due to their design and the use of specific functions.

The Contribution: Previous studies have predominately focused on passwords or the technical side of password managers [3,12–15] conducted general studies on password managers [9] or smartphone password managers [16,17], but rarely on the human perspective and user interface of password managers and types of password managers that are used. This paper looks at the user interface and usability of three cloud password managers using Nielsen's principles. Also, it looks at the human perspective regarding the use and non-use of password managers in regard to four key aspects—usability, trust, transparency and security—using an interview study and an online questionnaire study. This paper adds to the existing literature on the analysis of password managers using mixed methods to understand the obstacles to the adoption of password managers on the one hand, and the views of users of password managers on the other. In this paper, both expert and non-expert participants are compared in several aspects, such as password reuse and the use and non-use of password managers. Finally, this paper reports users' views on aspects such as trusting vendors, storing passwords, using random password generators and types of password managers that are used the most.

A previous study [18] only considered people with an educational background in information security as experts, or people that had many years of experience in this field [7]. In contrast, in the online questionnaire study, we expand the definition of experts and include people with an educational background related to computer science in the experts' group, while non-experts are those with a completely different educational background, such as journalism.

Research Questions:

1. Do current cloud-based password managers have suitable user interfaces and functions?

Explanation: The aim of using Nielsen's principles (heuristic evaluation) is to answer this research question. These principles (Section 3.1) are useful to identify and evaluate issues with the user interface and usability problems of a prototype and program. The evaluation of password managers will help us gain insights into the system and suggest solutions to improve its functions and user interface.

1. Are there any similarities in the reporting experience between users and non-users when using a cloud-based password manager?
2. Are there any similarities in the reporting experience between users and non-users in terms of trust and knowledge regarding password managers?

Explanation: The aim of the usability test and interview study (Section 3.2) is to answer these two questions. We aim to discover if there are any similarities between users and non-users in terms of ease of use, satisfaction and effectiveness when using a cloud password manager. In the interview section, the purpose is to find out if users and non-users of password managers have similar or different views of password managers in general, and if they see password managers as trustworthy and transparent tools. So, this study is not comparing password managers. Rather, it is comparing the views of users and non-users of password managers.

1. Does an education in computer science or information security play a significant role in adopting password managers and mitigating password reuse?
2. Do users of password managers have the same trust issues or security concerns as non-users?
3. Are there any differences between expert and non-expert users of password managers?
4. What are the reasons behind the low adoption rate of password managers among non-users?
5. Are there any differences between expert and non-expert non-users of password managers in terms of the reasons why they do not use them?
6. Are current password managers easy to use for users?

Explanation: The aim of the online questionnaire study (Section 3.3) is to answer the above six research questions and to ascertain whether an education related to computer science or information security increases the possibility of adopting a password manager and mitigating password reuse. Likewise, the aim is to find out if there are any significant differences between expert and non-expert users when using password managers, views on aspects such as storing all or some passwords, the use of random password generators and which types of password managers are used the most (cloud-based, browser-based, open source). Moreover, the aim is to determine if users of password managers, in big demographics, have trust issues and security concerns towards password managers like non-users, as well as find out if current password managers, for example, chrome and LastPass, are suitable for their users and which functions are difficult to use, such as recovering a password manager account. Additionally, for non-users of password managers, the aim is to explore the reasons behind the low adoption rate of password managers and to discover if there are any significant differences between expert and non-expert non-users as regards avoiding using password managers.

Hypothesis for Section 4.2.1:

1. There are similarities between users and non-users when using a cloud password manager.

Hypotheses for Section 4.3:

1. Having educational background related to computer science or information security play a significant role in adopting password managers and mitigating password reuse.
2. There are no significant differences between expert and non-expert users of password managers.

The rest of the paper is organized as follows: Section 2 Work related to this study, Section 3 Materials and methods, Section 4 Results of this study, which are divided into 3 subsections, Section 5 Discussion. Section 6 Implications for future research.

2. Related Work

A recent study [11] found that 41% of respondents include at least one piece of personal information in their passwords, such as a birthday, while others capitalize a letter to comply with password policy. A security researcher, Ciampa, analysed 32 million leaked passwords and found only 12% of passwords were 9 characters in length or longer [19]. Participants know that password reuse is not secure but is memorable [20] while 91% of participants reuse at least one of their passwords for multiple accounts [21]. The MTurk study [22] reported that participants reused on average 71% of their passwords, which confirms the result of prior work [23,24] that found that password reuse is rampant. Besides, 59% of participants reuse passwords for multiple accounts due to the difficulty of remembering long complex passwords [25]. Stobert and Biddle state that an attacker can gain access to several accounts if they discover one reused password [12]. However, a single password remains widely used for authentication [26]. As a result, password managers were developed to help people handle passwords safely and generate a unique password for each account.

A previous study [7] found that writing passwords down in a secure location or using password managers can be a promising solution for password reuse. Password managers offer the benefits of having strong passwords and uniqueness, compared to other entry methods [22], while they improve

usability by offering autofill login forms [27]. Moreover, password managers generate, store and encrypt passwords, while users need only remember one master password [28]; Komanduri et al. state that users create stronger passwords when they use memory aids, which can encourage them to use password managers [29]. In a study on the use of passwords among experts and non-experts, Stobert and Biddle found that the majority of non-experts use browser-saving features [30], while the majority of experts use a dedicated password manager and browser-saving features [18]. Also, the researchers [11] concluded that experts depend on many of the same coping strategies as non-experts, that is, reusing passwords and writing them down. Likewise, prior work [7] found that more experts than non-experts use password managers.

A recent interview study [31] found that users of browser password managers are driven by convenience, while users of separate password managers use them for their better security. In a study about the security practices of experts and non-experts [7], it was found that usability drawbacks of password managers are harder to deal with for non-experts, while suggesting that the low adoption rate of password managers might be due to an ingrained mental model. In a survey study on adopting and rejecting smartphone password managers [17], the results present a number of rejecting factors, such as usability, lack of awareness and trust, security concerns, device memory, battery and control. In a study on passwords [11], it was found that some participants do not use password managers because they do not trust them and are unwilling to install them. Additionally, Fagan et al. found that users of password managers have higher computer proficiency and better experience of computer security than non-users; they found that convenience, security and usefulness are the main reasons for using password managers by users, while non-users noted security and usability as the main reasons for not using them [9]. Similarly, it was reported that a lack of immediacy and time are the most common reasons for not downloading and using password management applications [32].

Gao et al. applied an ecological theory in a study on passwords which found that participants expressed fewer concerns about using password managers, such as the risk of password manager databases being hacked or accidental password loss [21]. Furthermore, Lyastani et al. state that the autofill functionality of the Chrome browser exacerbates the password reuse problem [22], while prior work [23,24] found that neither third-party password managers nor browser autofill significantly affected password reuse or strength. The results of various studies [22–24] show that password reuse and weak passwords have not been solved by current password managers.

To summarize, researchers [33] state that current password managers and browsers do not prevent password reuse, so this should be investigated further while preserving a positive user experience with password managers. Likewise, researchers [22] ask why users of password managers still employ weak passwords and reuse passwords, and they suggest further investigation to better understand and tackle the issues why users abstain from using password managers. One study [7] suggested making some usability improvements to password managers before recommending them to people, while other studies [23,24] state that the current forms of password managers might not be complete solutions. Stobert and Biddle [11] suggest integrating password managers into browsers and operating systems to help with trust and visibility. Also, a recent interview study [31] called for better design for password managers and more focus on non-expert users, as well as conducting further research to explore how education or advertising can target non-users of password managers and those with less technology experience. A recent study on smartphone password managers [16] found that mistrust is a strong reason for rejecting them, as they are barely acceptable, so there should be some improvements to security, guidance and interaction.

3. Materials and Methods

In this paper, heuristic evaluation using Nielsen's principles is conducted to gain insights into user interface design and the functions of three password managers; a usability test, an interview study and an online questionnaire study were conducted to explore the human perspective of using and not using password managers.

3.1. Heuristic Evaluation of Three Password Managers Using Nielsen's Principles

In the 1990s, Nielsen's 10 principles were developed as user interface design guidelines, which since then have been reflected in the design of products by companies such as Google and Apple [34]. According to Nielsen (1994), "in recent years, heuristic evaluation has seen steadily more widespread use, and many users of the method have developed their own sets of heuristics" [35]. Actually, Nielsen's principles (Table 1) [36] are useful and helpful to evaluate the design of programs and identify issues in user interfaces and usability problems that impact on the overall user experience. The evaluation is divided into two parts, a positive part for good points about a program, and a negative part where problems are identified and explained, along with recommendations to solve problems. Thus, the evaluation of password managers will help to gain insights into a program and its user interface and suggest solutions to improve it. Heuristics checklist can be found here [37].

An evaluator (not just any user) inspects the user interface and compares it to the heuristics so that they can list usability problems, then explain each problem and suggest solutions. The evaluation goes through four stages: training, evaluation, severity rating and debriefing. To the best of our knowledge, this study is the first evaluation of the user interfaces and usability of cloud-based password managers using Nielsen's principles. In this section, the researcher conducts an evaluation of three cloud-based password managers (LastPass, Dashlane and Keeper) using Nielsen's 10 principles. More precisely, the researcher evaluates the user interfaces of three password managers as well as their main functions, such as storing passwords, creating master passwords and recovering password manager accounts. The use of Nielsen's principles will answer the first question of this research: "Do current cloud-based password managers have suitable user interfaces and functions?"

Table 1. Nielsen's 10 principles and definition.

Visibility of System Status	The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
Match Between System and the Real World	The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.
User Control and Freedom	Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo.
Consistency and Standards	Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.
Error Prevention	Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
Recognition rather than recall	Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
Flexibility and Efficiency of use	Accelerators—unseen by the novice user—may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.
Aesthetic and minimalist design	Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
Help Users Recognize, Diagnose, and Recover from Errors	Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
Help and Documentation	Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.

The researcher evaluates cloud-based password managers because they have many features and functions; LastPass password manager is one of the most popular cloud-based password managers, it has many free features, can be used in multiple devices for free, and offers a recover account option using an authentication application. Dashlane and Keeper are also popular password managers with many features [16,38–41].

3.2. Usability Test and Interview Study

A usability test and a semi-structured interview study were conducted in Cardiff University, United Kingdom. Participants were recruited by sending emails to university staff members and students, and distributing brochures as well. In total, 30 participants responded to our email request and registered to take part in the study voluntarily. The 30 participants are from nine different schools, including computer science, engineering, law and journalism. The majority of participants are students[1].

Each participant completed the usability test using LastPass password manager, they did a number of tasks (Table 2) provided by the researcher, for example: create an account in LastPass, store an account/password, generate a password using a random password generator, enable multi-factor authentication, add a driving licence and recover a LastPass account. Regarding the seven tasks in this study, the idea for these tasks comes from a pioneering study by Chiasson et al. [10]. These tasks were also applied in another study [16,27]. The usability test has seven tasks because LastPass has many features and functions within it. None of the participants were asked to use their own passwords, email addresses or usernames. For the purposes of the study, usernames, email addresses, passwords and a master password were provided by the researcher to make the participants more comfortable during the usability test. The 30 participants used Windows 10 operating system to do the usability test, the versions of LastPass used during the study were between 4.31 and 4.36, but the change of versions did not affect the study at all. The interface of LastPass in the usability test was configured to English and the whole study took around an hour for each participant to complete.

Each participant was given a briefing information sheet which explains the purpose of the study, and after that they signed a consent form to participate. Likewise, participants were given a briefing sheet after finishing the study which contains a thank you message, explains what will happen to the results and how they can contact us in the future. Participants were asked a series of questions which were explained to them to ensure that they fully understood the questions. Participants were asked about their views on the interface design, language and usability of LastPass and about password managers in general during the interview. The researcher observed the participants during the usability test to ensure that any questions could be answered quickly, and to maintain a comfortable atmosphere for them as well. The researcher wrote down the participants' answers and comments during the usability test and interview study. The data for this study is stored in a secure place and treated with full confidentiality.

For the usability test, participants answered a set of questions about the use of LastPass using Likert scales, ranging from "1" strongly disagree to "5" strongly agree, and from "1" very dissatisfied to "5" very satisfied, and open-ended questions. After participants answered usability questions, they were asked another set of questions in the interview which were open-ended questions and direct closed-ended questions (Yes/No), they could add comments to justify their answers as well. The aim of this section of the study is to investigate any similarities between users and non-users when they use a password manager, if current password managers are easy to use, trusted and to what extent users and non-users are satisfied with and knowledgeable about them.

---

[1] A correction was made to the publisher's version where the following text was removed : "most of them are male (21 males and 9 females) and the age range is between 24 and 45 years old."

Furthermore, participants could test the usability of a password manager and give feedback regarding its design and functions. The reason for asking all participants to do the usability test before the interview was to let them practise and use an actual password manager in a monitored environment so that they could understand how it works, as there might be some participants who had never used a password manager or only used a browser password manager, so participants could see how to store passwords, change a master password and recover an account. Thus, the 30 participants could clearly understand the usability and interview questions, and the researcher could elicit some useful comments. Also, the main reason for choosing LastPass for the usability test is that it is the most popular cloud-based password manager, it has many features compared to other cloud-based password managers, it can be used on multiple machines for free, it is free to use the web page and browser extension with features and functions, and it provides an account recovery feature in case the master password is forgotten [16,38–41].

We conducted usability tests and interviews until no new answers or comments emerged, we also had a good sample size from each group. Participants' comments were analyzed using an inductive code approach [42] and codes were identified from the data. The researcher read through the participants' comments, generated a set of codes, refined them and finalised them. Please note that the closed-ended questions were analyzed quantitatively, while open-ended questions and comments were analyzed qualitatively. With regard to the number of participants required for the usability test, it was understood that five participants were needed to identify 80% of problems [43], while another study states that 10 participants are required to reveal 80% of problems and 20 participants to reveal 95% of problems [44]. In the usability test, we compared users and non-users by using three factors—easy to use, satisfaction, effectiveness (Table 3). However, we did not measure LastPass on a System Usability Scale (SUS) because the aim was to obtain answers about specific functions, which SUS does not offer. SUS provides one score for system usability, but it does not shed light on the problem itself and does not identify why a score is high or low. For example, SUS will not tell us if recovering a LastPass account is easy or hard, therefore we had to ask these questions directly without using SUS. In fact, we obtained many comments from participants about the LastPass user interface and its functions, thus we obtained more details about LastPass and its user interface.

Table 2. Seven tasks that were applied in the usability test.

Task 1—Initialization	Register and install LastPass browser extension. Participants first create an account and a master password in LastPass and install a browser extension for LastPass on the web browser they are using in the study.
Task 2—Password migration	Participants store a password and an account for a website in LastPass.
Task 3—Login	Participants log in to the website where LastPass has already stored the account and password in task 2.
Task 4—Change password	Participants use the random password generator in LastPass to generate a new password, after that they log in to the website and change the password. This task shows participants the security benefits of using a random password generator to generate a unique password for each account.
Task 5—Use some features	Participants search for specific features in LastPass to enable/add, such as driving licence, multifactor authentication, allow reverting to a master password, use the "Never URL page" and emergency contact. This task is included to see if participants can find these features and if they find them useful.
Task 6—Account recovery	Participants assume they forget the master password. They use a registered phone number and the LastPass authentication app to recover their account. Participants need to complete all steps for account recovery. This task was added to gain insights into how participants find the steps of recovering a LastPass account using multifactor authentication (easy or difficult).
Task 7—Remote-login	Participants log in to a password manager account (LastPass) from another computer using a registered email address and LastPass authentication app. This task was added to show participants how a password manager can be accessed from different machines and the benefit of synchronizing passwords.

Table 3. Definition of three factors used to compare between users and non-users.

Ease of use	Ease of using the system to complete tasks. 11 questions (Table 4).
Satisfaction	Design, language of the tool, overall experience and what is liked and disliked by participants (Table 5).
Effectiveness	Participant completes tasks accurately and successfully. (Did any participants not complete all tasks?) Which tasks could a participant not complete?

Table 4. 11 questions were answered by 30 participants about using LastPass and specific functions.

Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I find it easy to create an account in a password manager.	36%	57%	7%	0%	0%
I find it easy to use a password manager	10%	30%	47%	13%	0%
It is difficult to install the browser extension of a password manager.	3%	10%	27%	30%	30%
It is easy to store my online passwords in a password manager.	27%	47%	13%	13%	0%
I find it hard to change my online passwords in a password manager.	0%	20%	33%	37%	10%
I find it easy to access my online passwords that are stored in a password manager.	30%	47%	20%	3%	0%
It is easy to use a password manager on multiple devices.	17%	33%	20%	20%	10%
It is hard to reset the master password.	3%	20%	20%	30%	27%
It is easy to find and use random password generator.	7%	23%	33%	20%	17%
I find it difficult to recover my account if I forget my master password.	23%	20%	27%	23%	7%
I think I would need help/support to be able to use a password manager.	27%	10%	33%	20%	10%

Table 5. Three Questions Were Answered by 30 Participants about Their Satisfaction with Using LastPass.

Questions	Very Satisfied	Satisfied	Neither	Dissatisfied	Very Dissatisfied
How would you describe your overall experience with a password manager?	3%	60%	23%	7%	7%
How satisfied are you with language used?	10%	44%	20%	23%	3%
Question	**Excellent**	**Good**	**Average**	**Fair**	**Poor**
[2]What are your thoughts on the design and layout?	7%	13%	46%	27%	7%

Note: A correction was made to the publisher's version where the following text was removed : "of transparent password manager"

3.3. Online Questionnaire Study

We conducted an online questionnaire to include more participants and broader age and education level demographics. The questionnaire was designed using Google forms, which is a free service. To recruit participants, the online questionnaire was distributed via social media platforms such as LinkedIn and WhatsApp; also, the questionnaire was distributed across Cardiff university by email. After collecting the data, one repeated and two inconsistent answers were discarded; also, six users' responses were discarded because they stated that they use more than one password manager at the same time (two and four password managers), so we did not know which password manager they

meant when they completed the questionnaire; and in order to keep the study and analysis consistent and clear, we mapped each password manager to its user. Thus, the overall number of valid responses is 247. The data for this study is stored in a secure place and treated with full confidentiality.

The online questionnaire contains two parts, the first part targets all participants (general questions) while the second part has two sections; a section for non-users who do not use a password manager and a section for users of password managers. Please note that closed-ended questions (multiple choice, multiple options, Likert scale) were analyzed quantitatively, while open-ended questions were analyzed qualitatively. Different questions for users and non-users were used because the aim is to understand their perspectives on using and not using password managers. As for experts, the researcher [7] only considers people who have at least five years of experience in the security field to be experts, plus those who have a degree and work in computer security as experts [18]. In this study, we expanded the definition of experts by including people with an educational background related to computer science in the experts group, so participants who have a degree related to computer science or information security are considered experts.

In this section, we aim to discover whether an education related to computer science or information security increases the adoption rate for a password manager and helps to mitigate password reuse. Also, we aim to elicit views on aspects such as storing all or some passwords, the use of a password generator and which types of password managers are used the most (cloud-based, browser-based, open-source password manager). Likewise, the aim is to find out if there are any significant differences between expert and non-expert users in terms of trusting the vendors of password managers, and any security concerns. Moreover, the aim is to know if users of password managers, in big demographics, have trust issues and security concerns towards password managers as non-users, as well as find out if current password managers are suitable for their users and which functions are difficult to use, such as recovering a password manager account.

Additionally, for non-users of password managers, the aim is to discover the reasons behind the low adoption rate for password managers, even though they are widely available, and the most popular reasons chosen by them. Also, we want to find out if there are any significant differences between expert and non-expert non-users as regards not using a password manager. Please note that a few questions used in this study were taken from previous studies and adapted accordingly.

4. Results

This section is divided into three subsections: (1) heuristic evaluation of three cloud-based password managers, (2) usability test and interview study with 30 participants, (3) an online questionnaire about using and not using password managers with 247 participants.

4.1. Heuristic Evaluation of Three Cloud-Based Password Managers (LastPass, Dashlane, Keeper)

LastPass password manager: This is the most popular cloud-based password manager, it is free of charge and has many features. LastPass has its own web browser extension and webpage, so users are free to use either of them, but it is better to install the browser extension on a web browser to use the autofill feature. The evaluation of LastPass was conducted using free Windows version, v4.31.0 to v4.33.5.

Dashlane password manager: This is a cloud-based password manager that has its own application, browser extension and webpage. Dashlane has limited free features compared to LastPass. The evaluation of Dashlane was conducted using free Windows versions 6.1929.1 to 6.1935.0.

Keeper password manager: This is another cloud-based password manager which has its own application, browser extension and webpage. Keeper has fewer features than Dashlane and LastPass. The evaluation was conducted using free Windows versions 12.4.1 to 12.5.5.

4.1.1. Positive Aspects and Nielsen's Principles Applied to Three Cloud Password Managers

In this study of three cloud-based password managers (LastPass, Dashlane and Keeper), we found that they offer many features. These password managers store loads of passwords and categorize them, offer random password generator and store personal information such as "bank details". The system is visible as the menu of these password managers are the same, they provide concrete icons and speak the user's language with words and concepts familiar to the users. The three password managers use icons that match those in the real world such as payment, they have consistent grammars and terminology. They allow the user to copy and modify data, for example, the user can copy password and paste it on the log-in form which is also allowed on other pages. One of the features is autofill where the username and password are filled in automatically on a log-in form thus the user does not need to type them which saves time. Regarding changing sensitive date, they do not allow users to change sensitive data without asking them to enter the master password, otherwise the data are not changed. If there is an error, these password managers use a good text to inform users about errors which is shown briefly and unambiguously.

Moreover, the three cloud-based password managers provide the user with sufficient and understandable guidelines to use the system (Table 6). The random password generator generates a password once it is open and the user can change the length or remove characters. In LastPass and Dashlane password managers, user can use different paths to find functions, for example, account settings, which makes it flexible to open it quickly. Regarding password changer, only Dashlane provides this good feature as user can change a password with only one click because Dashlane will change the password on the website automatically, yet this feature is only available for specific websites. In Keeper password manager, users can recover the account by installing the application and follow few important steps to reset the master password which is easier than LastPass and Dashlane.

Table 6. Positive aspects and Nielsen's principles applied to three cloud password managers. Explanation of positive aspects can be found in the Appendix A.1).

Password Managers	Positive Aspects	Principles Applied
All 3	System display page	Visibility of system status.
All 3	Main menu of the system	Visibility of system status, Consistency and standards, Aesthetic and minimalist design.
All 3	Icons, grammar, and terminology	Match between system and real world, Consistency and standards.
All 3	Storing personal information	Visibility of system status, Flexibility and efficiency of use, User control and freedom.
All 3	Storing online passwords	Visibility of system status, Flexibility and efficiency of use, User control and freedom.
All 3	Main system page (vault)	Aesthetic and minimalist design, Visibility of system status.
All 3	Copy and modify data	User control and freedom, Flexibility and efficiency of use.
All 3	Autofill credentials to log in	Flexibility and efficiency of use, Recognition rather than recall.
All 3	Change sensitive data	Error prevention.
All 3	Random password generator	Flexibility and efficiency of use, User control and freedom.
All 3	Error messages (warnings)	Help users recognize and diagnose and recover from errors, Error prevention.
All 3	Log in to main page (vault)	Flexibility and efficiency of use.
All 3	Help section for users	Help and Documentation.
LastPass Dashlane	Different paths to find functions	Flexibility and efficiency of use, User control and freedom.

Table 6. *Cont.*

Password Managers	Positive Aspects	Principles Applied
LastPass	Account settings	Consistency and standards, Visibility of system status.
Dashlane Keeper	Tools/Settings	Aesthetic and minimalist design, Consistency and standards, Visibility of system status.
Dashlane	Password changer	Flexibility and efficiency of use.
Keeper	Recover account	Flexibility and efficiency of use, Help users recover from errors.

4.1.2. Problems, Violations of Nielsen's Principles and Severity Ratings for the Three Cloud Password Managers

There are few problems in LastPass, Dashlane and Keeper that might affect their adoption by people, particularly novices (people without any computer science background). The Table 7 below shows the problems, violations of principles and severity ratings.

The three password managers have few problems that might affect their adoption by people, particularly novices (people without any computer science background). We found that there is no undo function when the user enters a master password and confirms an important change such as changing email address or master password. Also, there is no undo function if a user removes a username or password from account details. The three password managers do not prevent a user from inserting incorrect data in a field or storing incomplete data, for example, store a wrong long URL. Another problem is that these password managers store different passwords for the same account with no prevention, so the user will end up with a duplicate account and will not be able to figure out which one is correct. The three cloud password managers use many computer jargon which will not be understood by all users, particularly novices. For example, they use "vault", "VPN" and "Breachwatch."

Additionally, the three password managers do not have asterisks (for mandatory) in data entry and dialogue boxes. In LastPass, account settings functions are not visible while Dashlane has dark colours for the main menu which might not be acceptable to all users. Importantly, users can create a master password that does not match the requirements in LastPass, users of Keeper can create a very weak master password for example, 123456, while users of Dashlane can create a master password that meets strong requirements but only by using an email address that registered in Dashlane. Significantly, recovering the account in LastPass is difficult as it has to be from the same device and browser and requires a smartphone, while Dashlane requires contacting the business team which is not free, yet, android users can recover Dashlane account using their own biometrics. Finally, we found that old passwords that we had changed during the evaluation are already stored and not permanently deleted from LastPass and Dashlane password managers which can be trust and transparency issues.

4.2. Usability Test and Interview Study

Before starting the usability test, we asked the 30 participants about password managers. Seventeen participants stated that they knew a little about password managers, six participants said they knew about them (a few were using one), while seven participants said they did not know anything about them. Surprisingly, a few of those who did not know about password managers were using one to save passwords but were not aware of its name, while some of those who knew about password managers were not using one. We asked our 30 participants if they used a web browser such as Chrome or Firefox to save passwords, to ensure we could categorize them correctly later as users and non-users. We found that 16 participants were users of password managers as 14 of them said they used Chrome as a password manager to save passwords, one user used Safari while another used LastPass password manager. At the same time, two users who used Chrome said that they used Safari along with Keychain to save passwords.

Table 7. Problems, violations of Nielsen's principles and severity ratings for LastPass, Dashlane and Keeper. Explanation of problems and recommendations can be found in the Appendix A.2, along with all figures "from Figure A1 to Figure A26").

Password Managers	Problems	Violated Principles	Severity
All 3	Recovery from a serious wrong function as there is no undo when saving new changes.	Help users recognize and recover from errors, User control and freedom.	4
All 3	No asterisks in data entry and dialog boxes mandatory.	Recognition rather than recall, Flexibility and efficiency of use.	2
All 3	The system does not prevent a user from inserting incorrect data in a field or storing incomplete data.	Error prevention, Help users recognize and diagnose errors, Flexibility and efficiency of use.	3
All 3	Store different passwords for the same account as there is no prevention.	Error prevention, Help users recognize and diagnose errors, Flexibility and efficiency of use.	3
All 3	The use of extensive computer jargon by the system.	Match between system and the real world.	3
LastPass	Account settings functions are not visible and not well organized.	Visibility of system status.	2
LastPass	Users can create a master password that does not match the requirements.	Error prevention, Help users recognize and diagnose errors.	5
LastPass	Auto change password does not work with many websites and is not visible.	Consistency and standards, Flexibility and efficiency of use.	2
LastPass	Inconvenience in generating a new password.	Flexibility and efficiency of use, Visibility of System Status.	2
LastPass	Recovering a LastPass account is difficult as it has to be from the same device and browser and requires a smartphone.	Flexibility and efficiency of use, Help users recognize and diagnose and recover from errors.	4
Dashlane	Dark colour used for main menu.	Visibility of system status.	2
Dashlane	Users can create a master password that meets strong requirements, but only by using an email address.	Error prevention, Help users recognize and diagnose errors.	5
Dashlane	Changing the master password while synchronization is disabled causes loss of data stored on other devices.	Flexibility and efficiency of use.	4
Dashlane	To recover an account in Dashlane requires contacting the business team and is "not free".	Flexibility and efficiency of use, Help users recognize and diagnose and recover from errors.	4
Dashlane	Users have to install the Dashlane app to register and use all its functions and features, because it is not available on the webpage or in the browser extension .	Flexibility and efficiency of use, Consistency and standards.	3
Keeper	User can create a very weak master password.	Error prevention, Help users recognize and diagnose errors.	5
Keeper	There is no random password generator in browser extension of Keeper.	Flexibility and efficiency of use.	3
Keeper	For free version, users can only use an application but cannot use browser extension nor webpage.	Flexibility and efficiency of use.	3

As for the other 14 participants, we found that the most used web browser was Chrome, followed by Firefox; and none of them used a web browser mainly/primarily to save passwords or had never saved passwords in web browser or another password manager program. For example, some participants considered themselves non-users because they occasionally stored a few unimportant accounts in a web browser, such as Chrome, while other participant non-users did not save passwords in a web browser or any other program at all. Thus, there were 16 participants who stated that they use a password manager to save passwords on a regular basis and considered themselves users,

while 14 participants considered themselves non-users because they did not save passwords in any password manager tools or occasionally stored a few unimportant accounts. Overall, we had 14 (47%) non-users and 16 (53%) users of password managers.

Please note that 29 participants used LastPass (a cloud-based password manager) for the first time and there was only one LastPass user who said that they were not aware of the features and functions that currently exist in LastPass and only used the LastPass extension to store and auto-fill passwords.

4.2.1. Results of the Usability Test (LastPass)

As stated in the methodology section, we conducted a usability test using LastPass password manager because we wanted to see our participants use an actual example of a password manager so that they would be able to clearly understand and answer our questions in this study. Also, we could then compare between users and non-users as regards password managers (using specific functions) and explore their opinions about these tool, their design and language (Tables 4 and 5).

For the first question about whether it is easy to create an account in LastPass password manager, the vast majority agreed as they found it easy to create an account, while only two participants neither agreed nor disagreed. During the usability test, the 30 participants were asked to download and install the browser extension of LastPass (task 1). We asked our participants about the difficulty of installing the browser extension of LastPass. Eighteen participants did not find it difficult while only four participants found it difficult. We asked the 30 participants if it was easy to use LastPass, 14 participants (47%) answered neutrally while 12 participants found it easy to use. The other question was about the ease of storing a password in LastPass vault (task 2), 22 participants found it easy to store a password in LastPass, while only four participants disagreed as they found it difficult.

The 30 participants were asked to use the random password generator in LastPass to generate a random password for an online account and change it on the website (task 4), after that they should update and check the new password in the vault of LastPass. So, we asked them how hard it was to change the password when using LastPass. Fourteen participants did not find it hard to change a password in LastPass while ten participants chose neutral. Also, nine participants (30%) found it easy to use the random password generator compared to 11 participants who found it hard to use. This question helped the participants as they could see how useful a random password generator is, as it can generate a unique password for each account. After that, the participants were asked how easy it was to access passwords that were stored in LastPass password manager. Only one participant found it hard to access stored passwords while 23 participants found it easy to access stored passwords.

In fact, LastPass password manager offers a good feature that allows its users to access their online passwords from the web page, browser extension and multiple devices for free. So, the 30 participants used LastPass on two different devices (computers) while doing the usability test (task 7). We asked the participants how easy it was to use LastPass on multiple devices, 15 participants found it easy to use LastPass on multiple devices, while nine participants disagreed as they found it difficult. The reason why nine participants found it difficult might be related to the use of email verification when using a new device to access a LastPass account, also the use of LastPass authentication app in order to let a new computer/device be trusted on the LastPass side. This task showed our participants how a password manager can be used on multiple devices and can synchronize passwords.

We asked the participants to reset the master password during the usability test. Only seven participants found it hard to reset the master password while 17 participants found it easy to reset the master password. Participants who found it hard to reset the master password stated that LastPass uses two different words in the process of changing the master password. Actually, LastPass uses "change" on the account settings page but "reset" on another page which confused them. Also, LastPass should show the master password during the creation and changing stages, because a few participants said they could not see what they typed.

As stated earlier, LastPass is one of the most popular cloud-based password managers because it offers many features, one of which is the ability to recover an account in case a user forgets the master

password (task 6). Please note that to recover a LastPass account, participants must follow a few steps, such as enabling multi-factor authentication using an authentication app, "LastPass authenticator", and a smartphone to receive an SMS code (the researcher provided a smartphone to all participants). Thirteen participants found it difficult to recover a LastPass account, while nine participants did not find it difficult. The difficulty of recovering an account was related to a big restriction applied by LastPass, because LastPass only allows its users to recover an account by using the same device and browser, and using an authentication app. Finally We asked the participants if they would need help and support to be able to use LastPass, 11 (37%) of them said they would need help to use it while nine (30%) disagreed. Please note that 29 participants used LastPass for the first time in this study.

Moreover, we asked the participants a few questions about their overall experience with LastPass, the language used and the design and layout so we could measure their satisfaction. We found that 19 participants (63%) were satisfied with the overall experience, but four participants were very dissatisfied or dissatisfied. We asked our participants about the language used in LastPass password manager. Sixteen participants (54%) were very satisfied/satisfied with the language used whereas eight participants (26%) were very dissatisfied/dissatisfied. Regarding the design and layout of LastPass, only 13% of participants rated the design as good while (46%) participants found it average.

As mentioned in the methodology section, we measured the difference between users and non-users using three factors—easy to use, satisfaction and effectiveness (Table 3).

- **Easy to use: Ease of Using the System to Complete Tasks.**

To find out if there was any significant difference between 16 users and 14 non-users when using LastPass, the means and p-values ($p < 0.05$) of 11 usability questions were analysed using a Mann Whitney test because we do not have confidence in the normality of distribution. Please note that the questions and answers of (3, 5, 8, 10, 11) were inverted during analysis in order to calculate the means. As shown in Table 8, we found that more users found LastPass easy to use compared to non-users, but the difference between the two groups was not significant (U = 84.0, p = 0.257, N = 30). Also, users did not find it difficult to install the browser extension of LastPass compared to non-users, but the difference was not significant (U = 66.5, p = 0.058, N = 30). Surprisingly, users found recovering a LastPass account more difficult compared to non-users; however, the difference was not significant between the two groups (U = 89.5, p = 0.355, N = 30). Similarly, non-user participants found it easy to access stored online passwords in LastPass compared to user participants, though the difference was not significant (U = 110.0, p = 0.951, N = 30). The results show that there were no significant differences between users and non-users when using LastPass password manager, which means that there are similarities between the two groups in their reporting experience for the 11 usability questions.

- **Satisfaction: Design, Language, Overall Experience and What Is Most Liked and Disliked by Participants (16 users and 14 non-users).**

When participants were asked about the thing they liked most (open-ended question), users mostly mentioned "save passwords", "manage passwords" and "security reason". Whereas non-users answered "save passwords", "manage passwords", "autologin" and "time-saving" (Table 9). Notably, no non-users mentioned anything related to security reasons. In contrast, the things disliked by users were "lack of flexibility", "complexity and ambiguity" and "security concerns", while non-users said "design and not user friendly", "lack of flexibility" and "not familiar to people". Again, no non-users mentioned anything related to security concerns, the same as users.

Table 8. The mean, Mann Whitney U value and *p*-value of each question for 16 users and 14 non-users (easy to use). Exact significance is displayed for this test [2*(1-tailed sig.)].

Questions	Mean of Users	Mean of Non-Users	U Value	*p*-Value (0.05)
I find it easy to create an account in a password manager.	3.44	3.14	81.5	0.208
I find it easy to use a password manager	2.56	2.14	84.0	0.257
It is difficult to install the browser extension of a password manager. (inverted)	3.06	2.36	66.5	0.058
It is easy to store my online passwords in a password manager.	2.94	2.79	99.0	0.608
I find it hard to change my online passwords in a password manager. (inverted)	2.44	2.29	103.0	0.728
I find it easy to my access online passwords that are stored in a password manager.	3.00	3.07	110.0	0.951
It is easy to use a password manager on multiple devices.	2.50	2.00	90.0	0.377
It is hard to reset the master password. (inverted)	2.88	2.21	74.0	0.120
It is easy to find and use random password generator.	2.06	1.57	87.0	0.313
I find it difficult to recover my account if I forget my master password. (inverted)	1.50	1.93	89.5	0.355
I think I would need help/support to be able to use a password manager. (inverted)	2.06	1.43	78.0	0.166

Table 9. Comments sample for the question "What do you like the most?".

Code	Sample of Comments
Save passwords (users)	• Saving password. • Easy to store and save many passwords. • Predict the password to memorise it on behalf of me. • useful as it can store loads of accounts. • Remember passwords
Manage passwords (non-users)	• Easy to manage my passwords • Easier with only using master password and save time. • Make life easy to use your online accounts.
Security reason (users)	• Multiple factor authentication. • Security wise. • It has more security to protect data.
Auto-login (non-users)	• Allowing me to autologin. • Convenience in login to account. • Autologin.

In order to find the differences between 16 users and 14 non-users, a Mann Whitney test was used to analyse the means of three satisfaction questions and *p*-values ($p < 0.05$). As shown in Table 10, user participants were more satisfied with the language used and their overall experience of LastPass than non-user participants, but the difference was not significant (U = 94.0, $p = 0.473$, N = 30). Users were more satisfied with the design and layout of LastPass compared to non-users, yet there was no significant difference between them (U = 91.0, $p = 0.400$, N = 30). The results show that there are similarities between users and non-users in the reporting of their experience of satisfaction.

Table 10. The mean, Mann Whitney U value and *p*-value of each question for 16 users and 14 non-users (satisfaction). Exact significance is displayed for this test [2*(1-tailed sig.)].

Questions	Mean of Users	Mean of Non-Users	U Value	*p*-Value (0.05)
How would you describe your overall experience with a password manager?	2.63	2.29	94.0	0.473
How satisfied are you with the language used?	2.50	2.14	94.0	0.473
What are your thoughts on the design and layout?	2.06	1.64	91.0	0.400

- **Effectiveness: Participant completes tasks accurately and successfully. (Were there any participants who did not complete any tasks?).**

During the usability test, a few participants could not complete a specific task, so they skipped it. Only one non-user participant could not complete task 4 (use a random password generator). Also, five participants could not complete task 5 (use some features), as these participants could not find the "add driving licence" and "tick revert master password" features while using LastPass, yet they successfully found other features such as "Never URL page" and "Emergency contact".

- **Participants' comments about LastPass password manager:**

Our participants made many comments about LastPass. The comments from our participants reflected their opinions of LastPass (Table 11), which may also apply to other cloud password managers. Participants found the design complex, not user friendly, and they have some security concerns. However, some participants said LastPass provides good security to protect account "security wise".

In the usability test, we found that most of participants found it easy to access and store passwords in LastPass, found it easy to install browser extension, while around half of participants found it easy to use the program even though 29 of them used it for the first time. Also, more than half of participants were satisfied with their experience and the language used in LastPass. However, a few participants found it hard to use the program on multiple devices as well as using random password generator. Interestingly, around half of participants found it difficult to recover the account which was related to the restriction applied by LastPass. Thus, LastPass should facilitate the way users recover the account in case they forget master password.

Moreover, 46% of participants found the design and layout average which means LastPass should improves the design and layout. Both users and non-users made similar comments about LastPass, which are that they liked saving and managing passwords while they did not like the design, colour, lack of flexibility and computer jargon. Also, participants stated that master password policy of LastPass is weak and they way to recover the account is strict. Finally, we found that the vast majority of participants completed all tasks and there were no significant differences between users and non-users regarding "easy to use" and "satisfaction" of LastPass (Tables 8 and 10).

Table 11. Comments sample about LastPass password manager.

Code	Sample of Comments
Complexity in the design	• Adding item should be under the bank accounts in the menu. • Adding icon should be in the top or in the menu. • Auto change password is like an error sign. • I thought auto change password is a warning message. • The menu of account settings like multifactor and Never URL should be in better colour. • The colour and font of Account setting menu should be bold and better, the font of multifactor authentication steps on the web page is not clear. • Dark menu and not clear layout. • Why there is bank details and payment feature in the menu if I don't ask for them, only the feature I add should be in the menu. • The window setting has lots of options and not clear colour. • No stars for mandatory or optional field.
Not user friendly	• It shouldn't ask me to install the extension again. • It should open the vault automatically. • The name vault is not clear, it should be MySpace and so forth. • LastPass used two terms which are different than each other (change and reset) which is confusing. • It is annoying to enter master password many times but I know why they do it. • Asking for another master password to update is paranoia. • There should be a show password in resetting master password. • The library of URL should be listed in the field with Amazon and Facebook.
Security concern	• I should be able to use another machine to recover my master password/account. It is secure but paranoia. • Recovering account, it is good and secure but if my PC is gone then I will not be able to retrieve my account. Overall, is not a good thing. • Accessing and recovering account is strict. It should be flexible. • What if I don't have the smartphone, what am I supposed to do. • Master password should have a strong policy.
Security wise	• It is brilliant to have verification from a new device even though it could lock me out. And it is a good thing too to use the app to add more security. • The app is worth it to secure my account. • It is higher security in securing the access to my account as no other computer can access my account. But it is complicated. • It is good to be asked to confirm master password many times.

4.2.2. Results of the Interview Study

After finishing the usability test, we started the interviews (semi-structured) with our 30 participants, asking them about password managers in general, thus we could find out if there are similarities between the two groups in terms of trust in and knowledge about password managers. Please note that the reason for asking all participants to do a usability test before the interviews was to let them use an actual password manager so that they could understand the idea of password managers, how they work and understand our questions, allowing us to elicit useful comments from them. The questions were used as guidance.

The following questions were open-ended questions and the answers were analyzed qualitatively. We asked our participants where would they expect to find a random password generator in a password manager. Thirteen participants (42%) said they would expect to find a random password generator in account settings, five participants said they expected to find it in the password dialogue box inside the vault, six participants said in the browser extension and five participants said on the main page of the password manager. We asked our 30 participants about the steps that they would take if a password manager failed and they could not access stored passwords. Eleven participants said they would call the help centre of the password manager company, six participants said they would enter their passwords manually for the websites they were using. Another six participants would use forget password for the website they wanted to access, while the other three participants stated that they would use the offline version of password manager. Also, only two participants said that they would

save their passwords in another place and one participant said they would close all password manager extensions and consider it a threat.

Moreover, we asked our user participants "why are you using a password manager?". Seven user participants use it to save passwords, six users use it for easy access to accounts, one user said to save time while two users use it for security reasons. Besides, we asked the 14 non-users the same question: what reason would make them use a password manager? Nine non-users said to save passwords, other participants said to manage passwords and have easy access, while one non-user said "If I used a password manager, I would say because of it is easy access". As our participants used LastPass, created and changed the master password during the usability test, we asked them about the technique they would use to save the master password of a password manager. Nineteen participants said they would memorize it, which means they know the importance of a master password. Ten participants would save it somewhere (on a smartphone or note), while one participant would use a hint to remember the master password.

The next set of questions were (Yes/No), the answers were analyzed quantitatively (descriptive) while participants' comments were analyzed qualitatively. We asked our participants if they checked the strength of the master password when they created it in LastPass and if they had any comments. Please note that we intentionally made a weak master password "h1234567" for the usability test to find out if our participants would pay attention to its weakness. Twenty-four participants said they checked the strength of the master password and the most relevant comments are: the master password in LastPass has a weak policy, not strong enough and less secure. Also, LastPass should require special characters and should have a strong and strict policy. One participant did not know if the master password was stored safely or not.

Besides, we asked the participants if they knew what would happen if the master was compromised. The answer from 28 participants was that they did know what would happen while only two participants answered "No" (one user and one non-user). When we asked our participants for comments, 23 participants stated that their stored passwords would be compromised if the master password was stolen. Other participants suggested using another layer of protection such as multifactor authentication to accept the log-in or reject it, they would use two-factor authentication to prevent any log-in from a different machine even though it is a headache. Likewise, one participant suggested that a password manager should provide a button for an emergency contact to shut down the account in case the master password was stolen.

During the usability test, the participants came across a feature called "emergency" which is offered by many password managers like LastPass, Dashlane and Keeper. This feature allows a user of LastPass (owner) to give a permission to another LastPass user (emergency contact) to access passwords in case the owner forgets the master password and cannot access their LastPass account. So, when we asked our participants if they would use this feature and add an emergency contact to recover stored passwords, 17 participants said "Yes", while 13 participants said they would not add an emergency contact. In detail, 14 users would use an emergency contact compared to only three non-users. Many participants gave some interesting reasons for not using this feature, for example, they trust no one, the emergency contact might get hacked so a hacker can access my account. One participant who would not use an emergency access said "I do not want to share my passwords with anyone". On the other hand, participants who said they would use an emergency contact stated that it is the best feature in a password manager, others said they would use it if it is free to add a personal account that belongs to them, while a few participants said they would add someone else they trust. One user participant who would use an emergency contact stated that "I would use it in case I die".

Furthermore, participants were asked a set of questions that related to the place and process of storing passwords in password managers, trust in storing passwords and deleting them permanently from password managers (Table 12). The 30 participants were asked if they know where online passwords are stored in password managers. We found that seven users out of 16 did not know where passwords are stored while nine non-users do not know. The most common comment made

by participants is that online passwords are stored on the provider's servers, other participants said they are stored somewhere in the cloud, while one participant said they are stored online in a database. So, these comments indicate that some participants were aware of storage places (provider's server and cloud). However, one user said passwords should be stored in a safe place and we should know how they are processed.

When we asked our participants about how passwords are processed in a password manager, most participants said they did not understand how password managers process online passwords. In detail, ten users of password managers and 11 non-users did not know the process. Nine participants said that stored passwords are encrypted while another user guessed that passwords should be encrypted and saved in distributed places (separately); for example, if we save five passwords, then three passwords will be saved in one place while the other two passwords will be stored in another place. Some of the participants who did not know the process stated that they could not see the process from the other side as well as they did not know what password managers do with passwords.

Additionally, we asked the participants if they would trust the browser extension to fill in passwords on their behalf, nine non-users and two users did not trust the browser extension to fill in passwords, so we can see that more non-users do not trust the extension to fill in passwords. A few participants who answered "No" said they would not trust the browser extension with financial accounts and would not use it for all websites. Likewise, other participants stated that they would not trust it because somebody else might use the browser and they would not trust the computer.

Table 12. Answers by 16 users and 14 non-users for (Yes/No) questions about password managers and the similarities between the two groups.

Questions	16 Users	14 Non Users
Do you know where a password manager store passwords?	Yes: 9—No: 7	Yes: 5—No: 9
Do you understand how a password manager process passwords?	Yes: 6—No: 10	Yes: 3—No: 11
Would you trust the browser extension of a password manager to fill in passwords?	Yes: 14—No: 2	Yes: 5—No: 9
Would you trust the vendor of a password manager to store all passwords?	Yes: 5—No: 11	Yes: 0—No: 14
Would you trust a password manager to delete password permanently from its database after you deleted it from vault?	Yes: 5—No: 11	Yes: 0—No: 14
Would you trust a password manager to retrieve account all time?	Yes: 15—No: 1	Yes: 12—No: 2
Do you know that a password manager synchronize passwords across devices using its own service?	Yes: 16—No: 0	Yes: 12—No: 2
Would you let a password manager store bank detail and passport information?	Yes: 3—No: 13	Yes: 0—No: 14
Would you install a browser extension of a password manager on a shared computer to access passwords?	Yes: 1—No: 15	Yes: 1—No: 13
Have you ever used a random password generator?	Yes: 3—No: 13	Yes: 2—No: 12
Do you know that chrome and firefox offer built-in password generator?	Yes: 5—No: 11	Yes: 0—No: 14

Surprisingly, only five users of password managers out of 16 would trust the vendor to store all passwords while 11 users and all 14 non-users would not trust it. This answer indicates that the majority of participants would not trust password managers with all their passwords. As a result, we asked our participants for a specific reason for not trusting the vendor. Many participants said that they did not store bank passwords in a password manager, while one participant said they did not want to depend heavily on a vendor. Another comment from participants who did not trust it was

"I do not know how they store it" and "I cannot trust them because they might access my accounts". On the other hand, there were user participants who trusted the vendor and said there was no other choice but to use it, while another said the vendor had a strong policy to store passwords. Also, one user participant said they would trust Chrome and LogMeIn because they are big companies, but one participant stated they would trust the vendor with some passwords but not with banking passwords. So, it can be seen that most of the comments are related to trust and security concerns (Table 13).

Table 13. Comments sample for the question "Trust the vendor of a password manager to store all passwords?"

Code	Sample of Comments
Trust issue	• Literally I do not trust them, especially if it is a bank password. Their employees might see the passwords, or they might get hacked from outside. • I cannot trust password manager with high priority passwords. • I have a trust issue if something happens to their server then it will be disaster. • I do not trust them. • I prefer to remember my passwords. • I cannot trust them with passwords particularly the important one.
Security concern	• There might be something happen to their servers and my passwords get compromised. • Because I will depend heavily on the vendor, so if something goes wrong, I will not be able to have my passwords. • I do not think it is safe.

We asked the users of a password manager if they store all passwords in it, 14 users out of 16 said they do not store all passwords. Surprisingly, three users who said they trusted the vendor to store all their passwords admitted that they did not trust the vendor with their banking passwords, so they do not store them. However, only two users stored all passwords in a password manager that they are using. Furthermore, 27 participants would trust the password manager to retrieve accounts/passwords all the time when they want to log in to online accounts. But only two non-users and one user would not trust it. One user who trusted it stated that they would not expect it to work if they use a new device which does not have a browser extension. However, one non-user said, "I would like this function if I used a password manager". When we asked our participants about password synchronization across devices, 28 participants knew that passwords are synchronized to other devices through the vendor's services.

We also found that 25 participants would not trust a password manager to delete passwords from its database after they deleted it from the vault. Please note that only five users of password managers trust it to delete passwords permanently, which implies that there is a lack of transparency and a trust issue towards password managers from both groups. Participants who replied "No" made a few comments that mostly related to trust and transparency issues, for example: "I do not trust them to delete my passwords", "they will keep the password even it appears to be deleted" and "I do not know what is happening in the other end". Another interesting comment is that "it is not possible to delete it technically because they have thousands of backups", "they cannot delete it, it is called digital footprint" and "I suspect they still have a copy of my password on offline storage".

Moreover, we asked our participants if they would let a password manager store their bank details and passport information, 27 participants said they would not let it store these details, while three users of password managers would store bank details and passport information. It implies that there are issue and security concerns toward password managers from both users and non-users. Three users who said they would let a password manager store their bank details and passport information stated that it is easy to access and store this data on Google Drive. A few participants who said "No" commented that they would not store it for a security concern, not safe for sensitive information and "if I use it, it will be for short time". Likewise, one participant said that they depend on themselves because they need greater security; another participant does not like this type of information being stored in another place, and a different participant said passport information is really important and if someone steals your account, then they have your information.

We asked our participants if they would install the browser extension of a password manager on a shared computer. Twenty-eight participants said they would not install a browser extension on a shared computer, while only two participants said they would do so (one user and one non-user). This answer means that participants from both groups would only use a password manager on their own computer/device but not on another machine that they do not own. Regarding these comments, many participants said if they put information on a shared computer, other people might access it and it is risky. Other participants said the machine might be compromised, as it might have malware. A small number of participants stated that they may forget to log out, while one participant said passwords will remain on the machine once synchronization happens.

Regarding the use of a random password generator, only three users of password managers and 2 non-users used a random password generator. When we asked participants for their reasons for not using a random password generator, many of them stated that they cannot memorize passwords as they are difficult to remember and they do not know them (Table 14).

As shown in Table 12, we found that user and non-user participants had similar knowledge and experience of password managers. Plus, their comments about password managers are similar, particularly in terms of trust and knowledge. The only difference we found is that most non-users do not trust a browser extension to fill in passwords, whereas the majority of users do trust a browser extension. An interesting finding is that many users and non-users do not know where passwords are stored, and they do not understand how password managers process passwords, which implies that there is a lack of transparency in relation to current password managers. The majority of users and all non-users do not trust password managers to store all their passwords or to delete passwords permanently from their databases, which means that both groups have a lack of trust in password managers. Similarities between users and non-users are also found in other answers; only one user and one non-user would install a browser extension on a shared computer, and the vast majority of users and non-users had never used a random password generator. Surprisingly, we found that the great majority of non-users were aware of password synchronization in password managers and trust password managers to retrieve their passwords all the time, which is similar to users of password managers. Astonishingly, only two users of password managers store all their passwords.

Table 14. Comments sample for the question "Have you ever used a random password generator?"

Code	Sample of Comments
Cannot memorize it	• I cannot memorise it. • long characters and difficult to remember. • I have no control of the password generator and cannot remember the passwords. • It is hard to remember. • I create it myself. Random generator is complicated and cannot memorize it. • Very large and difficult to remember. • It is complicated to remember.
Trust issue	• I do not trust the generator and cannot remember • I do not trust them.
Difficult to use	• I do not know how to use it. • I do not know how it works. • I cannot use it easily.

In the last part of the interview, we asked users of password managers if they reuse the same password on multiple accounts when they use a password manager. Shockingly, all 16 users of password manager said they reuse passwords in multiple accounts. When we asked non-users if they reuse passwords, 13 of them said they reuse passwords while only one non-user said "I have a system in my head to create password for accounts, every account has its own password and strong one". Users gave many reasons for reusing passwords, such as "it is easy to remember" and "I forget a lot". One user said I reuse password in case password manager fails to work. We asked our participants if they knew about built-in random password generators in web browsers (e.g., Chrome and Firefox). Only five users of a password manager knew about random password generators while 11 users and

14 non-users did not know. We asked them for comments and one participant said they never know, while one participant stated that they only knew about the Chrome browser. Also, two participants said they did not know about Chrome and Firefox, but they had seen a random generator in Safari web browser.

At the end of the interviews, some user participants provided some comments about password manager and suggestion to improve it. For example: "people start using it now, but we need to know how to store it in the cloud", "It is enough to save passwords and share between my devices that's what I need", "it is better to store my passwords in my own machine so I have control of it", "user interface functionality needs improvement, something just broken, something is not intuitive" and "for more security they should force you to update passwords".

Other user participants said "I want to have a password manager with more security", "make it more secure to satisfy users, use face scan or fingerprint to authenticate myself to password manager" and "password manager should take full responsibility of any damage that happens to my passwords such as losing money from bank and leak to my passwords due to an attack".

Similarly, some non-users made comments about password managers and mentioned a few reasons that made them not to use it. For example: "password manager is not safe to use", "I am afraid if my data is stolen, and I trust my memory.", "I trust my memory more than password manager", "I do not trust this software", "it is free service so I expect them to use my data so as a result in this case my passwords for like amazon will be handed to them, so they might access my accounts, someone else might get access to my accounts and so many times you heard of people hacking to servers and data leaked. I am suspicious of this service and I am trying to avoid all these things".

Non-users also said, "I would use it for accessing account easily, but I cannot trust it to store my passwords", "I do not care about it, I am not interested in technical side, I do not trust the technical side to have my data" and "I don't want to save my passwords in password manager. I want them to show how they encrypt passwords and explain it in the agreement and ensure me they do not use it in commercial advertisement or sell it to others or get leaked".

In this part, we found that most users used password manager mainly to save password and for easy access to accounts but the majority of them did not store all passwords in the program. We found that 28 participants knew the consequences if master password is compromised which means they know the importance of it. Surprisingly, we found that many users of password managers did not know where passwords are stored, most of them did not know how passwords are processed in password managers which are similar to non-users' answers. The reason is that they did not know what password managers do with passwords which implies that there is lack of transparency and trust. However, we found that majority of users trust the browser extension of password manager to fill in passwords while the vast majority of participants trust password manager to retrieve passwords all the time which means they found this feature useful.

Interestingly, 25 participants would not trust the vendor to store all passwords or to delete them permanently while 27 participants would not store bank and passport information in password managers. This finding indicates that there is a trust issue, security concern and a lack of transparency towards password managers as participants do not know what is happening in the other end. In addition, 28 participants would not install the browser extension on a shared computer and the reason is that shared computer might be compromised or they may forget to log out. Another interesting finding is that the majority of participants have never used random password generator because they cannot memorize passwords, difficult to use and do not know them, while all users and 13 non-users reuse their passwords in multiple accounts. Finally, we found that there are similarities between users and non-users in terms of trust and knowledge regarding password managers.

4.3. Online Questionnaire Study

The online questionnaire was completed by 247 participants. We found that 43% of our respondents were 26–35 years old, 25% were 36–45 years old and 22% were 18–25 years old.

Also, 2% were between the ages of 56 and 65 years while only 2 participants were 66 years of age or older. The highest level of education for our participants varies, the majority of participants are undergraduates (41%, 101 participants), followed by those with a master's (32%, 78 participants) or a PhD (11%, 28 participants), while the rest of the responses came from participants with secondary school education and some college. So, most of the participants are well-educated.

One significant question in this part is related to the participants' educational background. So, we asked our participants if their educational background included computer science or information security. The purpose of this question was to compare between users and non-users of password managers, and experts and non-experts. As shown below, 52% of participants have a degree (education) related to computer science or information security, while 48% have different educational backgrounds. So, we call those with an educational background related to computer science or information security experts, while the rest are non-experts. Thus, there are 128 (52%) expert participants and 119 (48%) non-expert participants in Table 15.

Table 15. Numbers of Experts and Non-experts in this study.

Experts	Non-Experts	Total
128 (52%)	119 (48%)	247 participants

As is known, companies government sectors rely on the Internet for various services, thus we have seen a rapid increase in the number of websites; consequently, each person will have dozens of accounts to manage, which means each account needs a password. So, we asked, "How many online accounts do you have?" and found that 76 (31%) participants had more than 21 online accounts, followed by 51 (20%) participants with 11–15 accounts, and 37 (15%) participants had 16–20 accounts (Table 16). To find out if there was any significant difference between experts and non-experts, we used a Pearson Chi-Square test. We found that there was a significant difference between experts and non-experts and the numbers of accounts they have X2 (5, n = 247) = 19.338, $p < 0.002$.

Table 16. Number of online accounts for 128 experts and 119 non-experts.

Online Accounts	Experts	Non-Experts	Total
1 to 5	2	17	19
6 to 10	18	20	38
11 to 15	23	28	51
16 to 20	22	15	37
21 or more	48	28	76
I do not know	15	11	26

Also, we asked the participants, "How many unique online passwords do you have?" and 137 participants (55%) stated that they had 1–5 passwords, 31 participants had 21 or more passwords for their accounts, 47 (19%) participants had 6–10 passwords and 14 participants did not know how many passwords they had. We compared between expert and non-expert participants regarding how many passwords they had to see which group had more passwords. As shown in Table 17, experts have more passwords than non-experts; for example, 23 experts have 21 or more passwords compared to 8 non-experts; on the other hand, 60 experts have 1–5 passwords compared to 77 for non-experts. To find out if there was any significant difference between experts and non-experts, a Pearson Chi-Square test was performed. We found that there was a significant difference between experts and non-experts and the numbers of online passwords they have X2 (5, n = 247) = 14.986, $p < 0.010$. So, having an education related to computer science or information security helps to mitigate password reuse as experts have more passwords than non-experts.

Table 17. Number of Passwords for 128 Experts and 119 Non-experts.

Online Passwords	Experts	Non-Experts	Total
1 to 5	60	77	137
6 to 10	29	18	47
11 to 15	8	7	15
16 to 20	0	3	3
21 or more	23	8	31
I do not know	8	6	14

The last question in this part is about the use of password managers. We asked our participants if they used any kind of a password manager and 134 (54%) participants answered "No" while 113 (46%) participants answered "Yes", so they use one. We found that the number of expert non-users was 66 (52%) while expert users numbered 62 (48%). The number of non-expert non-users was 68 (57%) while non-expert users numbered 51 (43%) Table 18. To see if there was any significant difference between experts and non-experts in adopting password managers, a Pearson Chi-Square test was performed. We found that there was no significant difference between experts and non-experts in adopting a password manager X2 (1, n = 247) = 0.774, $p = 0.379$. This finding shows that having an education related to computer science or information security does not play a significant role in the utilisation of a password manager.

Table 18. Numbers of Users and Non-users of Password Managers, including experts and non-experts.

Experts	Non-Experts	Total of Users
62	51	113 (46%)
Experts	**Non-Experts**	**Total of Non-Users**
66	68	134 (54%)

Moreover, we discovered that users of password managers had more passwords than non-users (Table 19). To see if there was any significant difference between users and non-users and their number of passwords, we used a Pearson Chi-Square test. The difference between users and non-users was significant X2 (5, n = 247) = 28.172, $p < 0.001$. Likewise, we found a significant difference between users and non-users and the number of accounts they have X2 (5, n = 247) = 18.395, $p < 0.002$.

Table 19. Number of Passwords for 113 users and 134 non-Users.

Online Passwords	Users	Non-Users
1 to 5	48	89
6 to 10	22	25
11 to 15	7	8
16 to 20	3	0
21 or more	26	5
I do not know	7	7

As seen above, we found that experts have more online accounts and passwords than non-experts and the difference is significant while there was no significant difference between the two groups in adopting a password manager. So, having educational background related to computer science or information security plays a role in mitigating password reuse.

4.3.1. Non-Users of Password Managers

In this study, there are 134 non-users of password managers, of which 68 (51%) participants have no educational background in computer science or information security (non-experts), whereas 66 (49%) participants do have an educational background related to computer science or information security, so we classified them as experts. Actually, expert participants are expected to adopt password managers because of their higher skills and knowledge of computer science than non-experts, yet, many stated that they did not use a password manager. The vast majority of non-users of password managers are well-educated, 41% of participants have a bachelor's degree, followed by 31% with a master's and 13% with a PhD. Also, 40% of non-users are aged 26–35 years, 28% are 36–45 years old while 21% are between the ages of 18 and 25 years.

- Reasons for not using a password manager

To understand why this group of participants were not using password managers, a list of 13 options (Table 20) was provided to them so that they could choose the reasons that applied to them or they could state their own reasons (they must choose at least one reason from the list or write a reason of their own). The reasons are related to the usability of password managers, trust, transparency and security. When we asked non-user participants about their reasons for not using a password manager, most of the reasons that were chosen related to trust issues, followed by security and transparency issues.

The reasons most selected by non-users participants related to trust issue, as 41.8% chose "I do not trust the vendor of a password manager to store my passwords" and 41.8% chose "I do not trust the browser extension of a password manager to fill in my passwords". Other reasons related to a lack of transparency in password managers, as 38.1% of non-users chose "I do not know where my passwords will be stored in a password manager", while 22.4% selected "I do not know how my online passwords will be processed in a password manager." Other participants chose reasons related to security concerns, as 35.8% chose "all my passwords will be leaked, if the database of a password manager is hacked" and 26.1% chose "If the master password is compromised/stolen, all my passwords will be exposed".

From the results, the main reason selected by non-user participants is that they do not use a password manager because they do not trust the browser extension or the vendor of a password manager, which means that non-user participants have trust issues regarding password managers. Similarly, non-users do not trust password managers to delete passwords permanently from databases. Another reason for not using a password manager is related to a lack of transparency, as non-user participants stated that they do not use a password manager because they do not know where passwords will be stored, and they do not know how passwords are processed in the database of a password manager. One more issue is that 20% of participants do not want to use password managers because passwords will be synchronized through the vendor's service.

Furthermore, many non-user participants have concerns about the security of the database of a password manager, which means that relying on a password manager to protect passwords can be risky. Non-users have concerns about the master password, because compromising the master password means all stored passwords may fall into the wrong hands. Similarly, 24.6% of non-user participants stated that other people who use the same shared computer could log in to their own password manager account. A tenth reason that causes non-users not to use a password manager is related to the availability of their stored passwords, because they will not be able to access stored passwords if a password manager fails to work (29.1%).

Table 20. Number of times each reason was selected by 66 experts and 68 non-experts, which also means these reasons were not selected by the remaining experts and non-experts. The table shows the overall time and percentage of reasons selected by both groups. A Pearson Chi-Square test was used to check for a significant difference between 66 experts and 68 non-experts for not using a password manager, it shows a Pearson Chi-Square value and a *p*-value for each reason selected/not selected by both groups.

Reasons	Experts	Non-Experts	Overall	Chi Value	*p*-Value 0.05
It is difficult to use a password manager.	6	14	20/14.9%	3.487	Not Sig 0.062
It is hard to update passwords.	1	6	7/5.2%	3.613	Not Sig 0.057
It is difficult to recover my account if I forget my master password.	12	12	24/17.9%	0.007	Not Sig 0.936
I do not trust the browser extension of a password manager to fill in my passwords.	30	26	56/41.8%	0.718	Not Sig 0.397
I do not trust vendor of a password manager to store my passwords.	38	18	56/41.8%	13.321	Sig $p < 0.001$
A password manager will not delete my password permanently from its database after I delete it from my account/vault.	18	14	32/23.9%	0.823	Not Sig 0.364
My passwords will be synchronized to my other devices using the vendor's services.	14	13	27/20.1%	0.091	Not Sig 0.763
I do not know where my passwords will be stored in a password manager.	28	23	51/38.1%	1.051	Not Sig 0.305
I do not know how my online passwords will be processed in a password manager.	15	15	30/22.4%	0.009	Not Sig 0.926
All my passwords will be leaked if the database of a password manager is hacked.	30	18	48/35.8%	5.250	Sig $p < 0.022$
If my master password is compromised/stolen, all my passwords will be exposed.	19	16	35/26.1%	0.480	Not Sig 0.488
People who use my computer will be able to login to my password manager.	14	19	33/24.6%	0.817	Not Sig 0.366
If a password manager fails to work, I will not be able to retrieve my online passwords.	23	16	39/29.1%	2.080	Not Sig 0.149

Importantly, the last reasons chosen by non-user participants from the list are related to usability, as only 14.9% chose "it is difficult to use a password manager" while 17.9% selected "it is difficult to recover the account if I forget the master password". These results show that non-user participants did not mainly abstain from using a password manager because of usability issues but rather due to trust issues, followed by a lack of transparency and security concerns toward password managers. However, only four non-user participants (non-experts) stated that they do not know what a password manager is, while one participant said that they could not be bothered to put in the work to make it happen. Overall, the reasons most chosen by experts and non-experts are related to trust when compared to security and transparency, while reasons related to usability were chosen least by both groups. Thus, we identified the reasons for the low adoption rate of password managers in numbers and percentages (Table 20).

To determine if having an education related to computer science or information security is an important factor in abstaining from using password managers for 66 expert non-users and 68 non-expert non-users (for choosing and not choosing 13 reasons), we performed an analysis using a Pearson Chi-Square test (Table 20). We found that there were no significant differences between expert non-users and non-expert non-users for 11 reasons as *p*-values were greater than 0.05. For example, "I do not trust the browser extension to fill in my passwords" was chosen by 30 experts

and 26 non-experts, and there was no significant difference between both groups for choosing/not choosing this reason X2 (1, n = 134) = 0.718, $p = 0.397$.

On the other hand, there were only two reasons out of 13 for which expert non-users selected them more than non-expert non-users; there are 38 experts compared to 18 non-experts who do not trust the vendors of password managers to store passwords, and the difference is significant X2 (1, n = 134) = 13.321, $p < 0.001$. Furthermore, there are 30 experts compared to 18 non-experts who fear that their passwords will be leaked if the database of the password manager is hacked, and the difference between both groups is significant X2 (1, n = 134) = 5.250, $p < 0.022$. Therefore, we can see that having an education related to computer science or information security only plays a minor role in not using password managers.

In addition, to see which category was selected the most by non-user participants, every three reasons were grouped in a category (Table 21) and a McNemar test was used to see if there was any significant difference between these categories. It is important to note that participants who chose a reason from both categories were excluded, for example, usability and trust, so only non-user participants who chose reasons from one category were counted. For example, if a non-user selected 1–3 reasons from the "usability category" but none from the "trust category", then the result of this non-user participant would be counted. A McNemar test was used as it only counts participants who selected options from one category and eliminates those who selected options from both categories.

Table 21. Every three reasons from Table 20 were grouped in a category. McNemar test was used to see if there was any significant difference between these categories.

Category	Reasons
Usability category	• I find it difficult to use a password manager. • It is hard to update passwords. • It is difficult to recover my account if I forget my master password.
Trust category	• I do not trust the browser extension of a password manager to fill in my passwords. • I do not trust vendor of a password manager to store my passwords. • A password manager will not delete my password permanently from its database after I delete it from my account/vault.
Transparency category	• My passwords will be synchronized to my other devices using vendor's services. • I do not know where my passwords will be stored in a password manager. • I do not know how my online passwords will be processed in a password manager.
Security category	• All my passwords will be leaked if the database of a password manager is hacked. • If my master password is compromised/stolen, all my passwords will be exposed. • People who use my computer will be able to login to my password manager.

The results show that there was a significant difference between the usability and trust categories, as shown by the McNemar exact p-value < 0.001 and test statistic = 26.30. (61 non-user participants chose only trust reasons and 16 participants only chose usability reasons, 25 participants who chose from both categories were excluded, while 32 participants did not choose from trust or usability category). Likewise, there was a significant difference between the usability and transparency categories as shown by the McNemar exact p-value < 0.001 and test statistic = 14.06 (47 participants chose only transparency reasons, 17 chose only usability, 24 participants who chose from both categories were excluded, while 46 participants did not choose from transparency or usability category). It was found that there was a significant difference between the usability and security categories as shown by the McNemar exact p-value < 0.001 and test statistic = 14.78 (48 participants chose only security reasons, 17 participants chose only usability reasons, 24 participants who chose from both categories were excluded, while 45 participants did not choose from security or usability category). The findings

show that usability is not the main reason for not a using password manager, rather it is the trust issue followed by transparency and security.

[3]We also used a McNemar test to see if there was any significant difference between the trust, transparency and security categories. We found that there were no significant differences between the trust, transparency and security categories as the McNemar exact *p*-value was greater than 0.05. There was no significant difference between the trust and transparency categories as shown by the McNemar exact *p*-value = 0.063 and test statistic = 3.947 (36 participants chose only trust reasons, 21 chose only transparency, 50 participants who chose from both categories were excluded, while 27 participants did not choose from transparency or trust category). There was no significant difference between trust and security categories as McNemar exact *p*-value = 0.059 and test statistic = 4.083 (31 participants chose only trust reasons, 17 chose only security, 55 participants who chose from both categories were excluded, while 31 participants did not choose from trust or security category). There was a similar finding between the security and transparency categories as shown by the McNemar exact *p*-value = 1.000 and test statistic = 0.021 (24 participants chose only security reasons, 23 chose only transparency, 48 participants who chose from both categories were excluded, while 39 participants did not choose from transparency or security category).

As seen above, when we compare between the four categories, we found that the most selected category is trust which implies that trust issue is a major problem that makes people not to use a password manager. It is followed by transparency and security categories as both categories have a similar number of selected times, yet, they were not selected as many as trust category. Also, we found that fewer non-user participants selected usability reasons (category) when compared with trust, transparency and security categories, therefore we can see that usability is only a minor issue for non-users. Moreover, we found that the difference between usability category and the other three categories (trust, transparency and security) is significant. However, we found no significant difference between trust, transparency and security category, yet, trust were selected the most by non-users.

Few non-user participants made a few comments regarding their reasons for not using a password manager. One participant said that they wanted to log in from any other machine without a password manager, another participant said they already use a simpler and more secure system while one non-user had never considered using a password manager because of believing that their passwords will not be obtained by anyone else.

We found interesting findings regarding non-users, trust reasons were the most chosen by non-users for not using password managers as they do not trust the vendor to store passwords. Followed by reasons related to lack of transparency as many non-users do not know where passwords are stored and how password managers process them. Also, non-users chose reasons that related to security such as passwords could be leaked from database because of an attack. Interestingly, we found that the least chosen reasons by non-users were related to usability which implies that usability is only a minor issue while trust, security and transparency are major issues which lead to the low adoption of password managers. Importantly, in regard to the difference between expert non-users and non-expert non-users, we only found a significant difference between them in 2 reasons out of 13 reasons. So, having an educational background related to computer science or information security only plays a minor factor in not using password managers.

4.3.2. Users of Password Managers

In this study, there are 113 users of password managers, of which 62 (55%) user participants have an educational background related to computer science or information security (experts), while 51 (45%) user participants have different educational backgrounds not related to computer

[3] Corrections were made to the publisher's version regarding the categories. In line 7 "usability" was replaced with "trust". In line 10, "transparency or usability" was replaced with "trust or security". In line 14, "usability" was replaced with "security".

science or information security (non-experts). The results show that more expert users use a password manager compared to non-expert users. The vast majority of users (82%) are well-educated, as 41% have a bachelor's degree, 32% have a master's and 9% are PhD holders. Regarding users' ages, 46% of users are aged 26–35 years, 20% are 36–45 years old and 24% are between the ages of 18 and 25 years. The user participants use password managers on different operating systems, 84 users use Windows, followed by Android (53 users), iOS (50 users), Mac OS (40 users) and Linux (10 users).

We asked 113 user participants about the password manager they use (Table 22). By far, the most used password manager is Chrome (46%), it is followed by cloud password managers LastPass (20%) and 1Password (9%). The results imply that more user participants adopt browser-based password managers such as Chrome rather than cloud-based password managers such as LastPass. The reasons might be related to the simplicity and ease of access to browsers compared to cloud-based password managers, which require installing a separate app and browser extension to use them. LastPass is the second most used, while it ranked first among other cloud-based password managers in this study. As seen in Table 22, a few more non-expert users than expert users use Chrome, while more experts use LastPass than non-experts. But eight experts use 1Password compared to two non-experts, while all KeePass users are experts, which implies that experts are more aware of cloud-based password managers and KeePass compared to non-experts.

Table 22. Types of password managers used by 113 users (62 Experts and 51 Non-experts).

Password Managers	Experts	Non-Experts	Total
Chrome	25	27	52—46%
LastPass	13	10	23—20%
1Password	8	2	10—9%
Safari	3	2	5—5%
Apple Keychain	1	4	5—4%
Dashlane	3	2	5—4%
KeePass	5	0	5—4%
Bitwarden	1	2	3—3%
Firefox	1	1	2—2%
McAfee	1	1	2—2%
HP Manager	1	0	1—1%
Overall	62	51	113—100%

We asked our user participants if they store all their passwords in the password manager they use; 58% of users do not store all their passwords, while 42% users do store all their passwords. The results shows that most of the users in this study only store some passwords online. With regard to experts and non-experts (Table 23), we found that 28 experts store all their passwords while 34 experts store some passwords. Nineteen non-experts store all their passwords while 32 non-experts store some passwords. To see if there was any difference between experts and non-experts in storing passwords in password managers, we used a Pearson Chi-Square test. We found that there was no significant difference between experts and non-experts in storing passwords in password managers $X2$ (1, n = 113) = 0.720, $p = 0.396$.

To find out in which password managers users store all their passwords, we analyzed the most used password managers. Thirty-four (65%) users of Chrome do not store all their passwords while only 18 (35%) users do store all their passwords. LastPass users who store all their passwords number 11 (48%), while 12 users (52%) only store some passwords. Similarly, six users of 1Password store some passwords while four users store all their passwords. There are three Safari users, three Dashlane and three Apple users who store some passwords, whereas three users of KeePass store all their passwords.

Table 23. 62 Experts and 51 Non-experts (113 users) who store all or some passwords.

	Experts	Non-Experts	Total
Store all passwords	28	19	47—42%
Store some passwords	34	32	66—58%

Furthermore, we asked the user participants if they use a random password generator to generate a password for each account (Table 24). Half of the users (51%) do not use a random password generator, 20% only use a random generator for specific accounts, while 29% use a random password generator for each account. This finding shows that half of the user participants do not use a random password generator for each account although it is offered within the tool. In regard to experts and non-experts, we found that 22 expert users use a random password generator for each account while 28 experts do not use them. Among non-experts, only 11 non-experts use a random password generator for each account while 29 non-experts do not use them. Using a Pearson Chi-Square test, we found that no significant difference between experts and non-experts as regards using a random password generator X2 (2, n = 113) = 2.682, $p = 0.262$.

Table 24. Sixty-two Experts and 51 Non-experts (113 users) who use a random password generator.

Using Random Generator	Experts	Non-Experts	Total
Use it for each account	22	11	33—29%
Use it only for specific account	12	11	23—20%
Do not use random generator	28	29	57—51%

In detail, we found that eight users of 1Password use a random password generator for each account. For LastPass, 12 users use a random password generator for each account, five users only use one for specific accounts while 6 users of LastPass do not use them. Chrome users use random password generators the least as 37 users do not use them while only seven users use a random password generator for each account. From these results, the random password generators of LastPass and 1Password are the most used among all password managers, as they can help to mitigate password reuse and weak passwords. On the other hand, the majority of users who use a browser password manager, for example, in Chrome, do not use a random generator or only use one for specific accounts.

More on this point, we asked user participants who do not use a random password generator to answer another question about their reasons for not using a random password generator; 19% of users did not know how to use a random password generator while 42% did not know that a password manager offers a built-in random password generator. Other users reported many different reasons, 19% said it is hard and complex to remember and type, 7% prefer to create passwords by themselves that are memorable, 5% stated "in case I cannot access the manager" and "I do not feel safe" and 3% reported that "I have never thought about it".

Moreover, we asked our user participants "Why are you using a password manager?" We found that 46% of users use password managers to store passwords because they cannot remember all their passwords, followed by 26% of users who said it is easy to log in and quick to get access. Only 17% of users use password managers because they are secure and protect their passwords. Also, 7% of users use password managers to generate a unique password for each account and to avoid reuse.

- Using password managers

To find out how easy it is to use password managers and their functions, we asked our user participants to answer 10 questions about the password managers they use. The questions are on a Likert scale of 1–5 (ranging from strongly disagree to strongly agree). As each participant has a different experience when using a password manager and some questions might not apply to them,

a not applicable (N/A) option was included, for example, some user participants may have never used a password manager on multiple devices. In this part, we analyzed different password managers which are browser-based (Chrome), cloud-based (LastPass and 1Password) and open source (KeePass) in Table 25.

Table 25. Analyzing 4 different password managers (number of users for each program).

Chrome	LastPass	1Password	KeePass
52 users	23 users	10 users	5 users

We found that all users of LastPass and KeePass and nine users of 1Password found it easy to create an account. Likewise, all users of KeePass and 1Password and 22 users of LastPass found it easy to store online passwords. Also, all users of KeePass, nine users of 1Password and 20 users of LastPass found it easy to use the program. The answers to the three questions indicate that those users of password managers found it easy to use the programs, and to store passwords as well.

As for installing the browser extensions of LastPass, KeePass and 1Password, the vast majority of users did not find it difficult to install the browser extensions except four users of LastPass who found it difficult. The great majority of users of LastPass, 1Password and KeePass found it easy to access their passwords except for two users of LastPass and one user of 1Password who chose neutral, so none of these users found it difficult to access passwords stored in these password managers. Similarly, only two users of LastPass need help to use the program. Furthermore, most users of LastPass, 1Password and KeePass found it easy to change passwords, but a few users of each password manager found it hard to change passwords. When we asked these users about using password managers on multiple devices, 14 users of LastPass, seven users of 1Password and two users of KeePass found it easy to use the programs on multiple devices. However, a few users of LastPass and KeePass found it difficult to use the programs on multiple devices.

We asked user participants about how hard it is to reset the master password in these password managers. Eight users of LastPass and two users of 1Password and KeePass found it hard to reset the master password. However, a few users chose “not applicable” for this question, which suggests that they had never tried to reset the master password. Importantly, one of the issues with current password managers is the difficulty in recovering the account when a user forgets their master password. User participants were asked about the difficulty of recovering their account if they forgot the master password, the result is that seven LastPass users, five 1Password users and three KeePass users found it difficult to recover their account when they forgot the master password. But nine users of LastPass and a few users of 1Password and KeePass chose “not applicable”, which means they have never forgotten their master password or never tried to recover their account, so they do not know how difficult it is. It appears that current password managers are easy to use and it is easy to store passwords and access them, but these password managers still have issues regarding their use on multiple devices and recovering accounts.

With regard to 52 Chrome users, we found that the great majority of users found it easy to use and to store passwords. Similarly, 67% of Chrome users found it easy to use on multiple devices, while only 12% did not find it easy. These results indicate that Chrome is well-known and accessible. Likewise, more than half of Chrome users (65%) found it easy to access their passwords in their browsers while only 14% of users disagreed as they found it difficult. However, only 31% of Chrome users found it easy to change their passwords, 34% neither agreed nor disagreed, while 29% agreed as they found it difficult to change their passwords in Chrome. Lastly, in this part, users always worry about forgetting their master password and it is the same problem with Chrome users. Please note that, a Gmail password can be considered as a master password because it gives access to a user’s email inbox, Google drive, account and so forth [45]. The results show that 48% of Chrome users found it difficult to recover their master password (Gmail password), while 23% disagreed as they found it easy to recover it.

- Trust and security of password managers

Previous studies on password managers did not primarily focus on users of password managers and stored passwords. In this study, we believe that there are many users of password managers who have trust and transparency issues and security concerns as regards the password managers they use (Table 26). Also, we wanted to find out if there was any significant difference between 62 experts and 51 non-experts via a set of questions about password managers. Please note that we used a Mann Whitney test to check for a significant difference between experts and non-experts (Table 27).

First, we asked user participants if they knew where passwords are stored in a password manager; the findings are that 51% of users of password managers know where passwords are stored, 30% of users do not know, while 19% are not sure about the location of stored passwords. We analyzed these results in depth to discover which groups of users know more about their stored passwords. Half of Chrome and LastPass users know where their passwords are stored, while five expert users of KeePass know the place of stored passwords. However, around half of users of Chrome and LastPass, four Safari users and 4 Dashlane users are not sure or do not about the location of stored passwords.

Table 26. Twelve questions were answered by 113 user participants about the password managers they use. A few users answered (N/A) to questions 3 and 9 (3%), question 10 (4%), question 12 (2%).

Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I know where my online passwords have been stored in a password manager.	18%	33%	19%	21%	9%
I fully understand how a password manager process my online passwords.	18%	18%	23%	34%	7%
I feel confident to use browser extension of a password manager to fill in my passwords.	19%	46%	22%	5%	5%
I trust the vendor of a password manager to store all my online passwords including my sensitive passwords.	12%	39%	24%	17%	8%
I worry about losing all my passwords that are stored in a password manager.	12%	38%	17%	25%	8%
I am aware that a password manager will synchronize my passwords across my devices using the vendor's services.	30%	42%	19%	7%	2%
I trust a password manager to delete my password permanently from its database after I delete it from my vault/browser.	14%	33%	25%	18%	10%
I fear that a password manager will fail to work or retrieve my passwords, so I store my passwords in a secondary place.	5%	20%	22%	38%	15%
I fear that all my passwords in a password manager will be exposed if my master password is compromised.	28%	37%	18%	11%	3%
I write my master password down and store it in a safe place.	8%	17%	9%	21%	41%
I have opened my password manager account on a shared computer.	4%	13%	11%	37%	35%
I would let password manager store my bank details and passport information.	13%	29%	10%	19%	27%

Similarly, we asked user participants if they knew how passwords are processed in password managers; 41% of users did not know how their passwords are processed at the other end, 23% were not sure, while only 36% of users fully understood the process. So, most users (64%) do not fully understand or are not sure how their passwords are processed in password managers. This finding implies that more work needs to be done to increase the level of transparency between users and password managers regarding storing and processing passwords. In detail, we found that half of Chrome users did not know how their passwords are processed, while half of LastPass users did not know or were not sure. Shockingly, no Dashlane users knew about the process while the majority of Safari and Apple (Keychain) users did not know or were not sure about the process. In contrast, six users of 1Password and four users of KeePass knew about the process.

We asked our user participants if they felt confident to use a browser extension to fill in passwords; 65% felt confident while 10% did not feel confident to do so. However, three non-expert users chose "not applicable", which implies that they do not use a browser extension (one Chrome, one Firefox, one Safari user). The vast majority of Chrome, LastPass and 1Password users feel confident to use a browser extension to fill in passwords, which means the browser extensions of password managers are useful for most users. One of the questions in the study is to see if users are aware of password synchronization using a vendor's service; 72% of users were aware of this while only 9% were not aware. We found that the majority of users of Chrome, LastPass, 1Password, Dashlane, KeePass, Safari and Keychain were aware of it.

Another question is about trusting the vendors of password managers to store all passwords. We found that 51% of users of password managers trust the vendors of password managers to store all their passwords while the other half of users either do not trust them or are neutral about it. This finding is surprising as around half of users do not trust or have little trust in vendors. As a result, password managers need to be more transparent about stored passwords to gain users' trust. In detail, we found that many users of Chrome, LastPass and 1Password trust the vendors to store all their passwords. In contrast, the other half of users of these popular password managers either do not trust them or have little trust in them. Also, three Dashlane users do not trust them while four Safari users are not sure about the vendors.

Moreover, another answer shows that users of password managers are concerned about their stored passwords; 50% of users of password managers are worried about losing all their stored passwords, while only 33% do not worry about it. The reasons for this result could be related to storing passwords in the cloud (3rd party), or to the lack of transparency as users do not see what is happening to their own passwords at the other end. In detail, we found that more than half of users of Chrome, LastPass, Safari and Dashlane were worried about losing their passwords stored in these password managers. However, a few users of KeePass were not worried about losing passwords, as all the passwords are stored locally on the machine and are under the user's control.

Additionally, we asked user participants if they trust password managers to delete their passwords permanently from their databases. The results show that 47% of users trust password managers, on the other hand 28% do not trust them at all, while 25% of users are not sure if their passwords will be deleted permanently. These findings indicate that 53% of users have trust and transparency issues regarding password managers deleting passwords because users do not see anything at the backend, so they do not know about their deleted passwords. In detail, many users of Chrome do not trust it to delete passwords from the database or are not sure about it, while many users of all the password managers either do not trust them or not sure if their passwords will be deleted.

When we asked our user participants about writing a master password down and storing it in a safe place, 62% disagreed while only 25% stated that they write a master password down and store it in a safe place. Only five users chose "not applicable" for this question. These findings indicate that the majority of users memorize their master password and know the importance of it. Likewise, we found that 53% of users did not store their own passwords in a secondary place because they did not fear the password manager might fail to work. However, 25% of users store their own passwords in

a secondary place. Most users of LastPass, 1Password, Dashlane and Safari do not store their own passwords in a secondary place. Yet, there are users of LastPass, KeePass, Dashlane and many users of Chrome who have this fear, thus they store their own passwords in another place.

Furthermore, 65% of users of password managers in this study worry that all their passwords will be exposed if their master password is compromised/stolen. This result indicates that users are aware of the importance of their master password. However, only 14% of users disagreed with this question, while three chrome users chose "not applicable". In detail, the great majority of Chrome, LastPass, Dashlane and users of other password managers worry about having their passwords exposed if their master password is compromised.

As for whether users open their password manager account on a shared computer, 72% of them had not opened their password manager account on a shared computer, while only 17% had opened it. From this result, we know that users are aware of the risk of using a shared computer. Notably, no 1Password, Dashlane or KeePass users had opened their password manager account on a shared computer, while only a few users of Chrome and LastPass had done so, which is much fewer.

Actually, many cloud password managers such as LastPass offer features whereby a user can store passport information and bank details, the same thing with Chrome which offers google drive. Thus, we asked users if they would let a password manager store their bank details and passport information; 46% would not let a password manager store these details, while 42% would let a password manager store them. To find out which password managers are trusted by their users to store bank details and passport information, we analyzed them individually. Most LastPass and Chrome users would not store their personal information, while no Dashlane users would store their information do so. On the other hand, eight 1Password users and all KeePass users would store this information.

Looking at Table 27, we found that there were no significant differences between 62 expert users and 51 non-expert users for 12 questions as p-values were greater than 0.05. For example, there was no significant difference between experts and non-experts in terms of knowing the location of stored password in password manager (U = 1544.0, p = 0.826, N = 113). Similarly, there was no significant difference between experts and non-experts in terms of trusting vendors to store all their passwords (U = 1491.5, p = 0.590, N = 113). As seen in Table 27, we can see that a few more non-experts know where passwords are stored in a password manager, and more of them trust the vendors of password managers to store all their passwords compared to experts. In contrast, more experts feel confident to use the browser extensions of password managers, trust password managers to delete passwords permanently and are aware of password synchronization compared to non-experts. However, the difference between expert users and non-expert users is not significant for using password managers, also for using a random password generator. Therefore, having an education related to computer science or information security does not play any important role in using password managers.

A few user participants made some comments, for example: "I only use password manager for unimportant accounts such as shopping websites", "I store my passwords in it because it is easy to login my accounts" and "I do not know how secure the password manager is, I just use it to remember my passwords and to not type my password every time when I log in to my accounts", and one participant wrote "I do not trust password managers, and thus I won't store the most important passwords in password management services".

In this part, we found that the most used password manager is the browser-based "Chrome" which may be related to the ease of access to browsers. Also, we found that more than half of users do not store all passwords in the password manager they use while half of users do not use random password generator at all. The reasons for not using random generator are that users do not know how to use it as well as they do not know password managers offer a built-in generator. Interestingly, 46% of users use password managers to store passwords while 26% use it for easy to access which indicates that most of them do not use other features. Regarding expert users and non-expert users, we

found no significant difference between them in using password managers which implies that having education related to computer science or information security does not play any significant factor in using password managers.

In regard to the usability of password mangers, we found that the users in this study found password managers easy to use, easy to access and store passwords. However, many users found it difficult to recover the account when they forget the master password. So, we can see that password managers are easy to use but issue related to recovering the account should be solved. Moreover, we found that many users of password managers have security concerns about using a shared computer, worrying about losing stored passwords and the consequences of having the master password compromised. Significantly, around half of users have trust issues towards the vendor of password managers regarding storing all passwords and deleting them permanently. Similarly, many users have transparency issue with password manager regarding the place of stored passwords and the process. This finding answers the question on whether many users have the same trust issues and security concerns as non-users.

Table 27. Comparing 62 Experts and 51 Non-experts regarding using password managers. Using a Mann-Whitney test to find the means and significant difference (p-value 0.05) between the two groups.

Questions	Experts	Non Experts	U Value	p-Value 0.05
I know where my online passwords have been stored in a password manager.	2.26	2.33	1544.0	Not Sig 0.826
I fully understand how a password manager process my online passwords.	2.02	2.08	1538.5	Not Sig 0.800
I feel confident to use browser extension of a password manager to fill in my passwords.	2.76	2.60	1354.5	Not Sig 0.390
I trust the vendor of a password manager to store all my online passwords including my sensitive passwords.	2.24	2.39	1491.5	Not Sig 0.590
I worry about losing all my passwords that are stored in a password manager.	2.42	1.98	1267.5	Not Sig 0.060
I am aware that a password manager will synchronize my passwords across my devices using the vendor's services.	3.00	2.80	1378.0	Not Sig 0.215
I trust a password manager to delete my password permanently from its database after I delete it from my vault/browser.	2.29	2.18	1526.0	Not Sig 0.743
I fear that a password manager will fail to work or retrieve my passwords, so I store my passwords in a secondary place.	1.52	1.75	1381.5	Not Sig 0.231
I fear that all my passwords in a password manager will be exposed if my master password is compromised.	2.72	2.90	1378.0	Not Sig 0.463
I write my master password down and store it in a safe place.	1.19	1.37	1310.5	Not Sig 0.381
I have opened my password manager account on a shared computer.	1.03	1.24	1386.0	Not Sig 0.236
I would let password manager store my bank details and passport information.	1.82	1.82	1518.0	Not Sig 0.942

5. Discussion

In this paper, we have analyzed the user interfaces and functions of three cloud password managers, we have analyzed data from the users of specific password managers, such as Chrome,

LastPass and 1Password; we have also gained insights into why non-users do not use these tools and conducted an interview study with users and non-users to understand, in depth, their thoughts about password managers.

The findings of this paper are that current password managers are generally easy to use. The heuristic evaluation of LastPass, Dashlane and Keeper (Section 4.1.1) shows that they have a consistent design, provide concrete icons and terminology, offer a section to store personal information and passwords, offer autofill for credentials to log in and provide a built-in random password generator. In the usability test of LastPass (Section 4.2.1), the results show that there were no significant differences between users and non-users when using a cloud-based password manager; more than half of participants did not find LastPass difficult to use. Actually, they found it easy to store, access and change passwords, even though 29 participants used it for the first time. Also, 46% of participants in the usability test found the design and layout of LastPass was "average", while 27% found it "fair". Similarly, the results of the questionnaire study (Section 4.3.2) show that users of password managers found it easy to store and access passwords and it is easy to use password managers on multiple devices. Overall, current password managers are easy to use and users can familiarise themselves with them after using them a few times.

However, based on the findings of heuristic evaluation study (Section 4.1.2), cloud-based password managers should reduce the complexity of their design because the more features they have, the more complex they become; thus users, particularly non-experts (novices), will find it hard to use and adopt them. Cloud password managers should avoid using computer jargon so that they are easier to use and are adopted by more people, they should facilitate the process of recovering an account in case a user forgets their master password. Also, a few participants in the usability study (Section 4.2.1) did not like the colour and design, they found LastPass not user friendly and the process to recover the account is strict. Likewise, a few users of LastPass and 1Password in the questionnaire study found it difficult to recover the account. So, based on the comments and answers from participants in the usability test and our findings in the heuristic evaluation study, we call for a better design of cloud password managers for all users, which is in line with References [10,31], also, we call for less use of computer jargon and reducing the features in password managers, leaving options for users to add. We found that a browser-based password manager, for example, Chrome, is used the most, which may be related to its simplicity and ease of access compared to cloud password managers, which require the installation of a separate application and browser extension, as well as not all features being free. This finding about the use of Chrome was suggested by Stobert and Biddle [11], as they called for integrating password managers into browsers.

In addition, most users of password managers (Section 4.3.2) use them mainly to store passwords and to log in quickly, which implies that they use them for convenience but not for security reasons. The same was found in the interview study (Section 4.2.2), where most users used password managers to store passwords and for ease of access. These findings suggest that users in both studies (Sections 4.2.2 and 4.3.2) do not use the other features of password managers or might not be interested in them. Regarding random password generators, we found that half of the users in the questionnaire study and the vast majority of participants in the interview study did not use a random password generator because they did not know how to use it, they were not aware of it or they could not memorize a long complex password. Thus, password managers should make password generators visible within their systems so that users can find them and use them easily; also, they should produce memorable and strong passwords. This finding explains the reason behind the reuse of passwords in the questionnaire and interview studies (Sections 4.2.2 and 4.3.2).

Moreover, it was found that having an education related to computer science or information security does not necessarily increase the adoption of password managers, plus we found no significant differences between experts and non-experts for adopting and using password managers. So, education does not play a significant role in using or not using password managers (Section 4.3), which we assume it is related to people's view about these tools. In contrast, it was found that education is an

important factor in reducing password reuse as experts have more passwords than non-experts, yet, many experts still reuse passwords, which is in line with a study [11] where experts follow the same strategy as non-experts for reusing passwords. Also, users in the questionnaire study reuse passwords for multiple accounts, particularly Chrome users, which is in line with a study in References [22–24], while users of LastPass and 1Password use random password generators which shows that cloud-based password managers can help to reduce password reuse.

Furthermore, we found that the main reason for the low adoption rate of password managers among non-users was due to issues related to trust, which was the reason most selected by non-user participants (Section 4.3.1). We also found that all non-users in the interview study did not trust the vendor of password managers. Thus, Non-users in both studies (Sections 4.2.2 and 4.3.1) do not trust the vendors of password managers to store passwords or to delete them permanently. So, trust is the main reason not to use a password manager. More to the point, a new finding is that the lack of transparency between non-users and password managers forces non-users to refrain from using these tools because the majority of non-users in the interview study and non-users in the questionnaire study did not know where passwords are stored, or the process of storing passwords. Likewise, security concerns about the databases of password managers and master passwords are another important reason that make non-user participants do not use password managers. The security concern finding is in line with the study in References [9,17,21]. However, the low adoption rate for password managers is not because of usability issues or lack of awareness, as suggested by References [9,17], but mainly due to trust and transparency issues, along with security concerns.

Additionally, it was discovered that around half of users in the questionnaire study (Section 4.3.2) and the majority of users in the interview study (Section 4.2.2) have trust issue towards the vendors of password managers, and so most of them do not store all their passwords. Similarly, many user participants in both studies (Sections 4.2.2 and 4.3.2) mentioned a transparency issue towards password managers regarding the location of stored passwords, and the process as well, because they cannot see what is happening to their passwords. These findings answer the question on whether many users have the same trust issues and security concerns as non-users, hence, password managers should explain the process more and let users interact with the system to increase the level of trust between them; at the same time, password managers need to be more transparent about stored passwords to gain users' and non-users' trust and increase adoption.

Besides, most users of different types of password managers (Section 4.3.2) have security concerns about master passwords as well as worrying about losing their stored passwords in password managers. The worries about master passwords are justified, because in the heuristic evaluation study (Section 4.1.2), we found that the current policy for master passwords in three password managers (LastPass, Dashlane, Keeper) is weak and does not prevent users from creating weak and guessable passwords. For example, LastPass does not force its users to create a strong master password that matches requirements, while Keeper allows its users to create a very weak master password that is easy to guess. Likewise, participants in the interview study (Section 4.2.2) stated that the master password policy in LastPass is weak and so it should apply special characters and have a strong and strict policy. Finally, the findings of our study imply that more work needs to be done to increase the level of trust and transparency between people (users and non-users) and password managers.

6. Implications for Future Research

The findings of this paper show that usability is not a major issue, it is issues with trust, transparency and security of password managers that compel non-users not to use them, while users have the same issues and concerns as well. It can be seen that password managers (cloud-based, browser-based, open source) are easy to use, yet, cloud password managers should improve their design and layout, avoid using computer jargon and reduce complexity in recovering accounts. In fact, there are dozens of password managers that have been developed by companies, while many researchers proposed password managers to solve issues related to usability and security,

for example, storing passwords securely on a smartphone while decryption keys are stored in a different place [13,14]. According to Alkaldi and Renaud [46], there has been no solution that encourages people to use password managers and enhances trust up until now.

Consequently, there is a need to find a solution that bridges the gap between people (users and non-users) and password managers. We argue that trust and security concerns can be solved if password managers become more transparent and show people what is happening to their stored passwords. Improving transparency in password managers can facilitate understanding, allowing people to interact with the system can help to motivate them to start using a password manager and enhance their trust, because when something is visible, people will realize how trustworthy it is. In our future work, we intend to investigate the impact of improving the transparency of password managers.

Limitations: The usability test and interview study (Section 4.2) were conducted at a university (small demographic) with the vast majority of participants being students. However, the study was extended by conducting an online questionnaire (Section 4.3) to include more participants, both users and non-users, with difference education levels and broader demographics. Also, the usability test only focused on LastPass; as a result, user participants in the questionnaire were asked to answer a set of questions based on the types of password managers they use. For the heuristic evaluation (Section 4.1), we evaluated three cloud-based password managers because they have many features, functions and user interfaces that can be tested.

Author Contributions: Methodology, F.A.; Formal analysis, F.A.; Investigation, F.A.; Resources, F.A.; Writing—original draft F.A.; Supervision, G.T. and P.R.; Review and editing, G.T. and P.R.; All authors have read and agreed to the published version of the manuscript.

Funding: The researcher Fahad Alodhyani (F.A.) is funded by Majmaah University, Saudi Arabia.

Acknowledgments: The authors would like to thank the 30 participants who took part in the usability test and interview study, as well as the 247 anonymous participants who completed the online questionnaire study.

Conflicts of Interest: The authors declare no conflict of interest.

Ethical Approval: The usability test, interview study and online questionnaire were reviewed and approved by the Ethics Committee of the School of Computer Science and Informatics at Cardiff University, UK.

Appendix A. Heuristic Evaluation Results of Three Cloud-Based Password Managers (LastPass, Dashlane, Keeper)

Appendix A.1. Explanation of Positive Aspects in the Three Password Managers

System display page: The main page of LastPass has a title which lets the user know which page they are browsing. Dashlane's main page does not have a title or header, but there are enough instructions and information in the middle of the page to let users know which page they are on and what it is about. The main page of Keeper has a title and there are enough instructions and information on the page to inform the user which page it is.

Main menu of the system: The menu is the same across the three password managers, it has the same colour and background. If a user chooses a specific page, the icon of that page will be active while other icons are greyed out. So the system status is visible, the menu design is consistent and aesthetic. Keeper offers many different colours for the menu so the user can choose and change them.

Icons, grammar, and terminology: The three password managers provide concrete icons across the system as well as speaking the user's language with words and concepts familiar to the user. The icons used match those in the real world, such as payments.

Storing personal information: There are many dialogue boxes which have an entry data field in the system. Each dialogue box has its own fields and requires information which is easy to populate by users. For example, the driving licence entry field has different requirements to the bank account field.

Storing online passwords: There is a specific dialogue box for each account/password, the user can fill in accounts and passwords, categorise them into groups and choose preferred options for accounts. Also, the user can store account details and passwords automatically by allowing the browser

extension to save credentials when logging in to the website in the future. Please note that LastPass provides a list of URLs in its library, so the user can choose from them.

Main system page (vault): The main pages of the three password managers have good layout and design (concise and aligned), this is where a user can categorise stored data and use a grid view or large view to organize them. When the user adds new information or changes it, the system will show a notification.

Copy and modify data: The three password managers allow the user to copy password and paste it on the log-in form and in a dialogue box, the same thing is allowed on other pages (across the system). So, data can be modified and saved easily to save time.

Autofill credentials to log in: The three password managers provide their users with an autofill feature where the username and password are filled in automatically on a log-in form, so the user does not need to type these, which saves time. If the user has multiple accounts on the same website, then the system will show a drop-down list of accounts so the user can choose an account from the list.

Change sensitive data: The three password managers do not allow users to change sensitive data without asking them to enter the master password; otherwise, the data are not changed/updated, thus any errors are prevented, which keeps the user's sensitive data safe from being changed, for example, changing a phone number or resetting a master password.

Random password generator: When a user opens the random password generator, the password generated is already shown to the user. The user can change the length of the password and/or remove characters. Also, the user can use a random password generator from the website itself (e.g., Twitter) and fill in old and new passwords. Dashlane shows the strength of a password generated in words and colours (unlike LastPass). However, Keeper only has a random generator embedded in the password section, so it is not a separate tool as in LastPass and Dashlane.

Error messages (warnings): The three managers use very good text to inform users about errors, an error message is shown briefly and unambiguously and does not criticize the user for anything.

Log in to main page (vault): The three password managers open the main page (vault) to the user once the correct username/email and master password are submitted on the log-in form (webpage), thus the user does not have to look for the vault elsewhere.

Help section for users: The three password managers provide the user with sufficient and understandable guidelines to use the system. Instructions are divided into different sections.

Different paths to find functions (LastPass/Dashlane): The random password generator can be found in different places. This makes it flexible to open it more quickly. Also, users of LastPass can find the account settings from other paths.

Account settings (LastPass): The majority of settings and features are presented in one place. The user can navigate the account settings and choose a function or feature. Each feature/function will be active when the user clicks on it (red underline).

Tools/Settings (Dashlane/Keeper): The majority of settings and features are presented in one place. The user can navigate the account settings and choose a function or feature. Each feature/function will be active when the user clicks on it. [4].

Password changer (Dashlane): This is a good feature in Dashlane as a user can click on a stored password and then on "change", after that Dashlane will change the password on the website automatically on behalf of the user. Note: this feature is only available for specific websites, such as the IMDb website.

Recover account (Keeper): Users can recover an account by installing the application on a computer, after that they click on forget password. Keeper will send a verification code to the registered email and then ask the user to answer a security question. Finally, the user will reset the master password and again access the account without losing any passwords.

---

[4] A correction was made to the publisher's version where the following text was removed : "(red underline)"

Appendix A.2. All Figures, Explanations of Problems and Recommendations in the Three Password Managers

Recovery from a serious wrong function as there is no undo when saving new changes: In the three password managers, if a user removes a username or password, then there is no undo function for it. Also, if the user enters a master password and confirms the operation, they will not be able to undo it, which is serious if changing a master password or email address. Recommendation: the three password managers should allow users to undo any functions within a specific time, for example, 24 h, so that they can rectify a mistake that might have been made (severity: 4-Major).

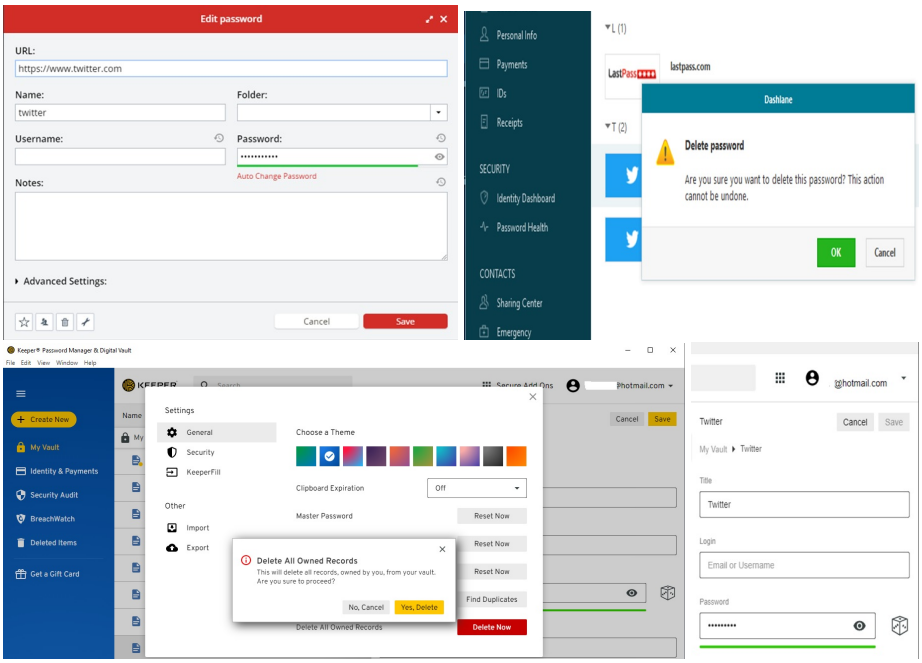

Figure A1. Remove username from LastPass. Remove password from Dashlane and save the changes without the undo function. There is no undo for deleting all records and username in Keeper (personal email is hidden).

No asterisks in data entry and dialogue boxes mandatory: Users will be confused about which data they need to fill in. Recommendation: The three password managers should use asterisks for mandatory fields that need to be filled in, such as names, email, ID and so forth, so it is clear to all users (severity: 2-Cosmetic).

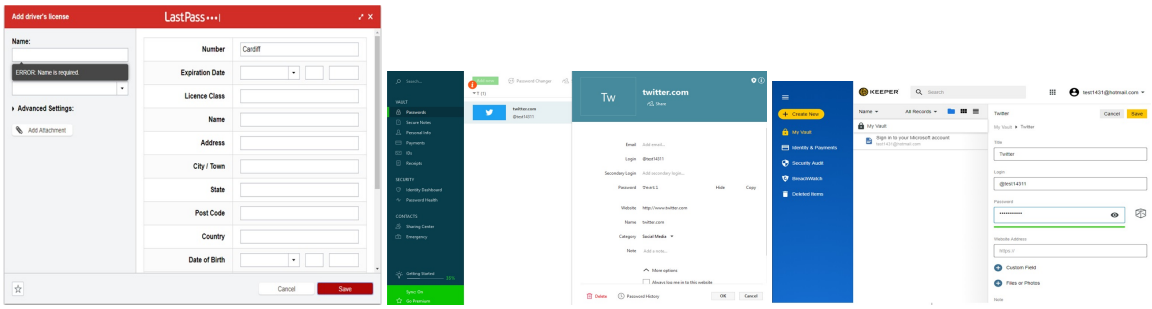

Figure A2. Data entry forms in LastPass, Dashlane and Keeper, which do not have asterisks. Part of password in Dashlane is hidden.

The system does not prevent a user from inserting incorrect data in a field or storing incomplete data: The three password managers do not prevent a user from storing incorrect data in a field, such as storing numbers in an alphabetic field. It allows a user to store a wrong long URL and an incorrect long phone number. Recommendation: The three password managers should

prevent users from inserting incorrect URLs, long wrong phone numbers and incorrect email addresses (severity: 3-Minor).

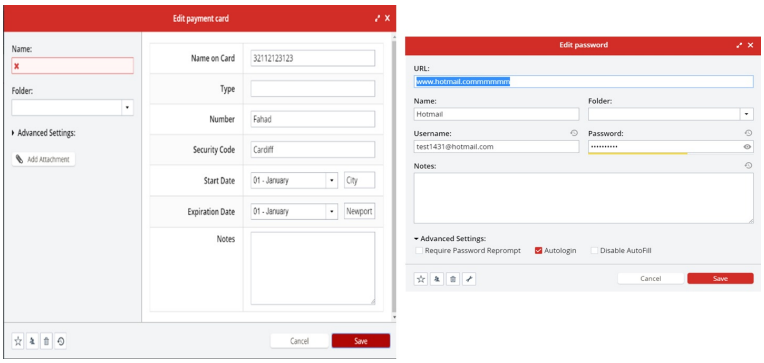

Figure A3. LastPass does not prevent users from storing wrong data, for example, incorrect URL, alphabetic instead of numerical characters.

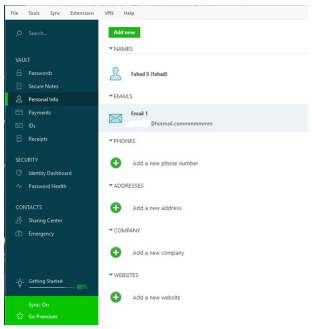

Figure A4. Dashlane does not prevent users from storing wrong data, for example, incorrect email address. The personal email here is hidden but you can see the wrong extension of @hotmail.commmmmmm.

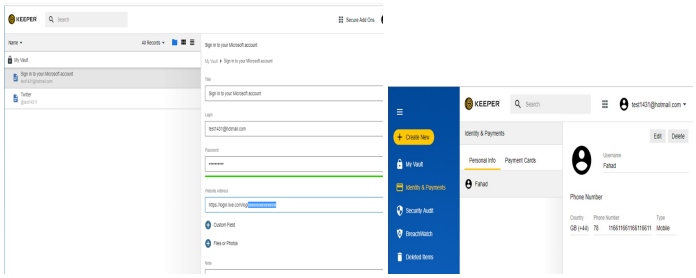

Figure A5. Keeper does not prevent users from storing wrong data, for example, incorrect URL and phone no (part of phone number is hidden).

Store different passwords for the same account as there is no prevention: These password managers allow a user to store different passwords for the same account. So, when a user wants to log in to a website, they will end up with a duplicate account with different passwords and be unable to figure out which one is correct. Recommendation: The three password managers should delete an account that has an old password and keep an account with a new password, or at least grey out an account with an old password (severity: 3-Minor).

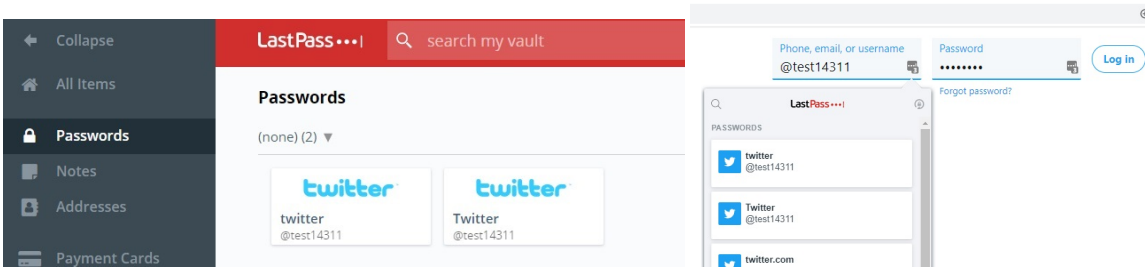

Figure A6. LastPass does not prevent users from storing different passwords for the same account "Twitter". The account can appear twice on the autofill log-in "Twitter website".

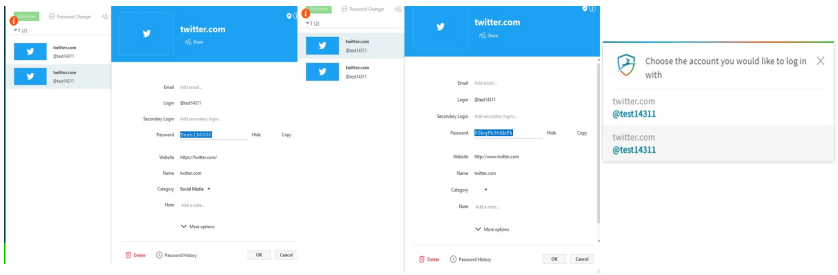

Figure A7. Dashlane does not prevent users from storing different passwords for the same account.

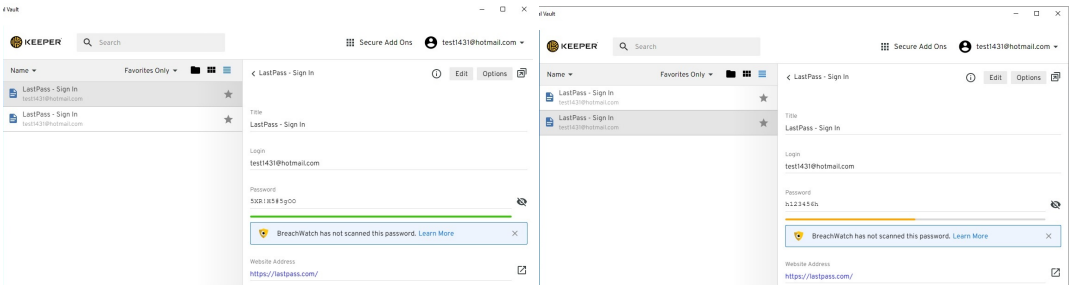

Figure A8. Keeper does not prevent users from storing different passwords for the same account.

The use of extensive computer jargon by the system: The three password managers have extensive computer jargon which will not be understood by all users, particularly novices. For example, "Vault", "Sync" and "PBKDF2" are ambiguous words for many users, along with "Equivalent Domains", "Breachwatch" and "VPN". Plus, LastPass uses different words for the same function; for example, when a user wants to change a master password, a new page opens and says: "Set master password". Recommendation: The systems should consider novice users and avoid using jargon, or provide explanation for jargon on the page (severity: 3-Minor).

Figure A9. Computer jargon (Account Settings in LastPass).

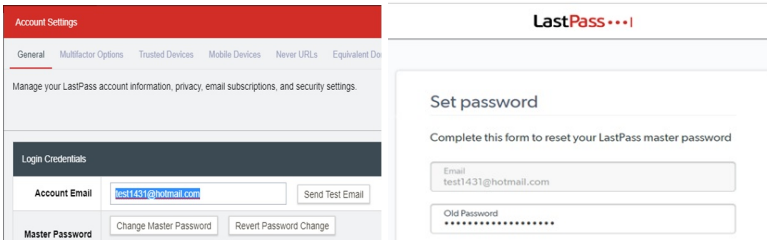

Figure A10. LastPass use different words for the same action, change master password and set master password (no consistency).

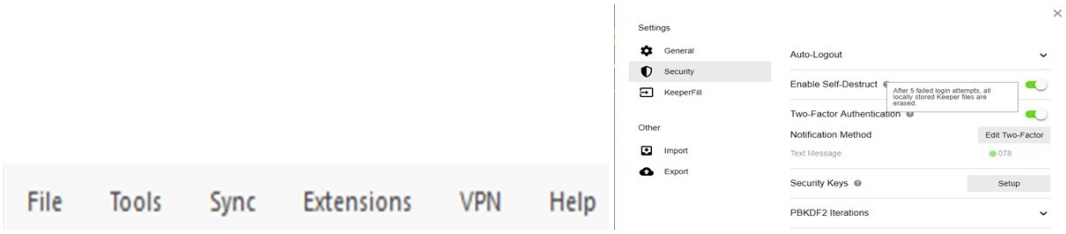

Figure A11. Computer jargon used in Dashlane and Keeper (part of phone number is hidden).

Account settings functions are not visible or well organized (LastPass): This might not be acceptable to all users, especially when using grey. The colour of account settings is not clear for all users. Recommendation: LastPass should use better and visible colours that suit all users (severity: 2-Cosmetic).

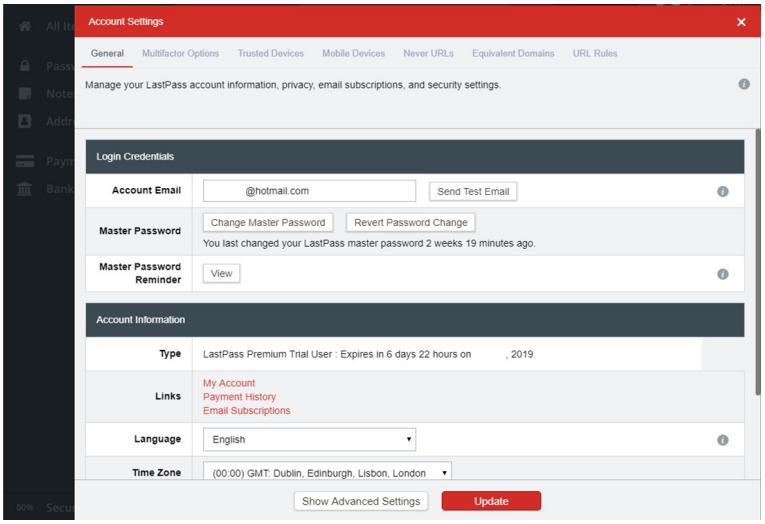

Figure A12. Colour of LastPass (Account Settings). Personal email and date are hidden.

Users can create a master password that does not match the requirements (LastPass): It does not prevent users from creating a weak master password that does not match the requirements and allows it to be used in the system, which is risky. Recommendation: LastPass must use a stronger policy and prevent users from creating a master password that does not match the requirements (severity: 5-Catastrophic).

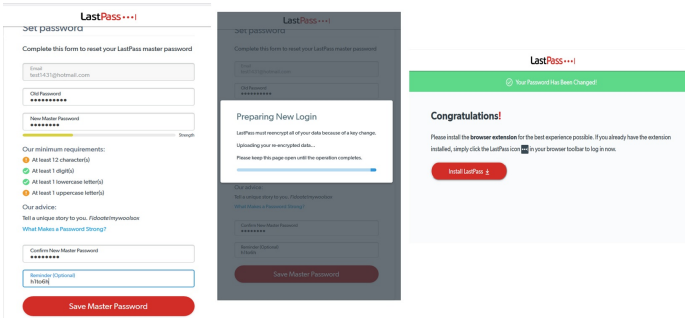

Figure A13. LastPass allows users to create a weak master password that does not match its policy.

Auto-change password does not work with many websites and is not visible (LastPass): It does not work for many websites such as Twitter, this feature is not available for websites such as Hotmail, the button is not visible to all users because it looks like an error message. Recommendation: LastPass should show a list of websites for which passwords can be changed, similar to Dashlane's password manager (severity: 2-Cosmetic).

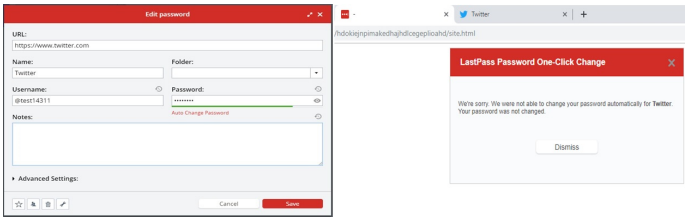

Figure A14. Auto-change password does not work in LastPass.

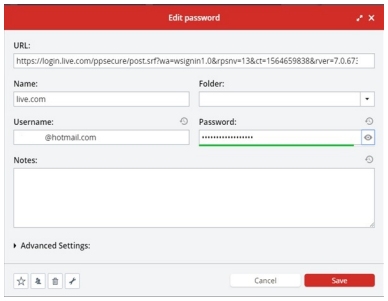

Figure A15. Auto-change password in LastPass does not support all websites, for example, Hotmail. Personal email is hidden.

Inconvenience when generating a new password (LastPass): Users have to figure out how to use the random generator because there is a lack of instructions, it does not show the strength in words (only in colours), so novice users might find it inconvenient to use it to generate passwords. Recommendation: LastPass needs to label weak and strong, which will be helpful for all users (severity: 2-Cosmetic).

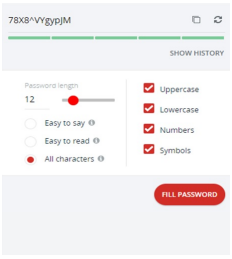

Figure A16. Random password generator for LastPass.

Recovering a LastPass account is difficult as it has to be from the same device and browser and requires a smartphone (LastPass): If a user forgets the master password, they must use the same computer and the same browser, and install a browser extension, to recover the account, plus use a smartphone app for the recovery process; otherwise, the account will not be recovered and all data will be lost, except if emergency access is used. Recommendation: LastPass needs to alter the way users can recover an account to only using an authentication app, because using the same device and browser, and installing an extension, is a big restriction to complete the process of recovering an account (severity: 4-Major).

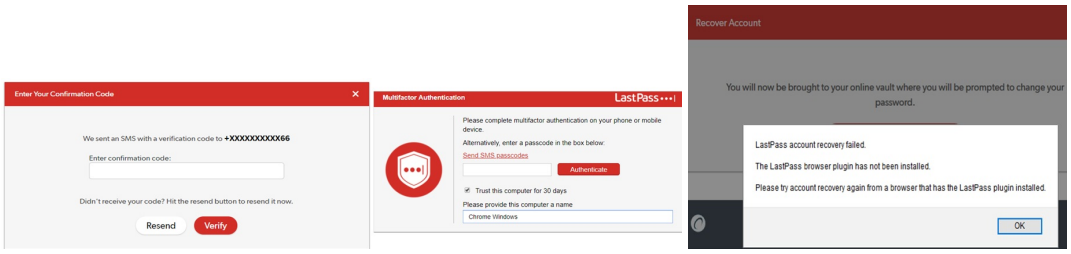

Figure A17. Requires SMS code and authentication app. Also, recovering a LastPass account is very strict as users must use the same device and browser.

Dark colours used for the main menu (Dashlane): This might not be liked by all users, especially when using dark colours for the menu and a small font. Recommendation: Dashlane should use better and brighter colours for the menu that suit all users (severity: 2-Cosmetic).

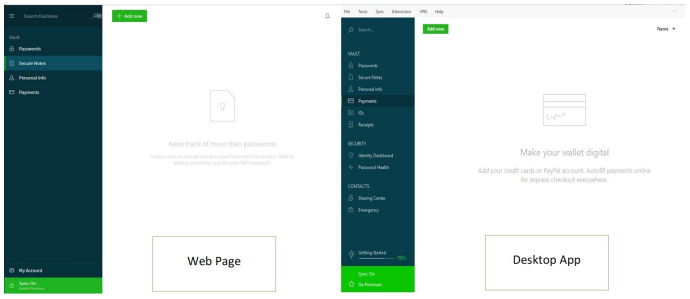

Figure A18. Colour of application and webpage of Dashlane.

Users can create a master password that meets strong requirements, but only by using an email address (Dashlane): It imposes a strict master password policy on users (at least 8 characters, 1 uppercase, 1 lowercase, 1 number); users have to follow this policy, otherwise they will not be able to complete registration. However, users can use an email address which is registered in Dashlane as a master password. The only thing that needs to be changed is replacing a lowercase letter with an uppercase and adding a number. Recommendation: Dashlane should prevent the use of an email address as a master password, and prevent the use of names of users, birthdays and any registered personal information (severity: 5-Catastrophic).

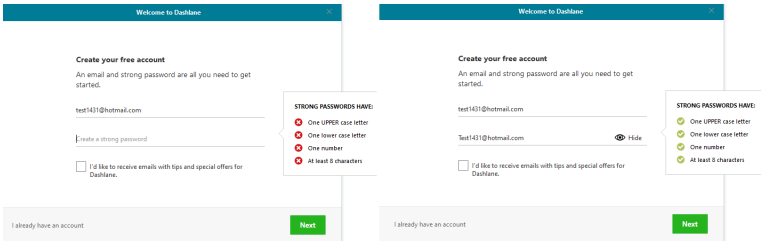

Figure A19. Users of Dashlane can create a master password using their email address.

Changing the master password while synchronization is disabled causes a loss of data stored on other devices (Dashlane): Users have to be careful when they want to reset the master password because if they do not have a premium membership and change the master password, then all data stored on other devices will be lost. Recommendation: Dashlane should make this feature "free" for at least one extra device to encourage people to adopt it (severity: 4-Major).

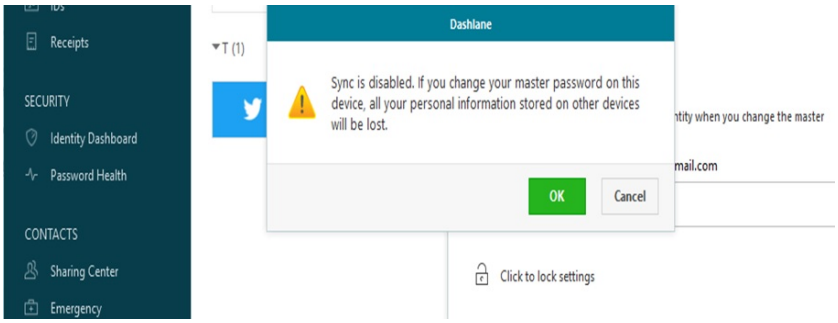

Figure A20. Changing the master password while synchronization is disabled causes a loss of data stored on other devices.

To recover an account in Dashlane requires contacting the business team and is "not free" (Dashlane): Unlike LastPass, users have to have a business membership to be able to recover an account through a third party, or add an emergency contact who can recover passwords; otherwise, users will not be able to recover data if they forget the master password. Please note that Android users are able to recover their account using their own biometrics. Recommendation: Dashlane should allow users of all devices to recover their account using an authentication app, SMS code or sending a code to a registered email address (severity: 4-Major).

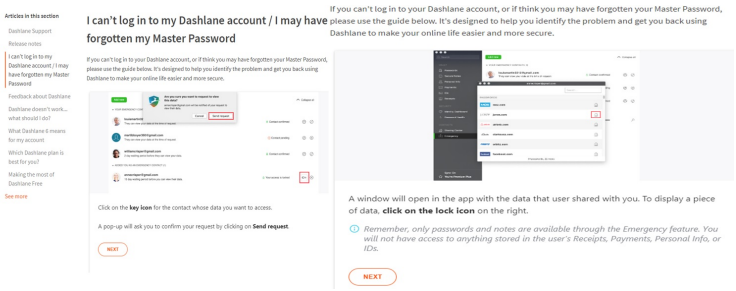

Figure A21. Recovering a Dashlane account requires a business team membership (not free).

Users have to install the Dashlane app to register and use all its functions and features, because it is not available on the webpage orin the browser extension (Dashlane): Users have to install the application to use specific features and functions because the webpage and browser extension do not have these features and functions. Recommendation: Dashlane should add important features to the webpage and browser extension, similar to LastPass, and for free, so that users do not have to install a separate app on their devices (severity: 3-Minor).

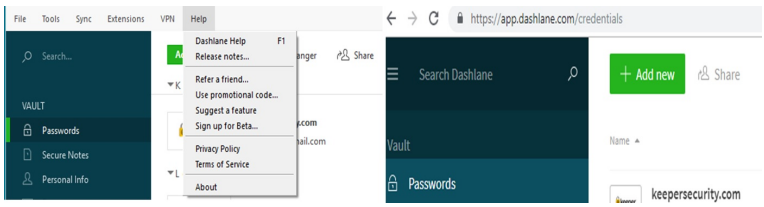

Figure A22. The application has all the features and functions, while the webpage does not.

User can create a very weak master password (Keeper): It does not impose a strict master password policy on users (at least 6 characters long); thus, the user can create a very weak password for example, 123456. Keeper does not show any master password policy when the user creates a master password for the first time, or when resetting the master password. Recommendation: Keeper must act and fix this as soon as possible by applying a strong master password policy and imposing it on all users (severity: 5-Catastrophic).

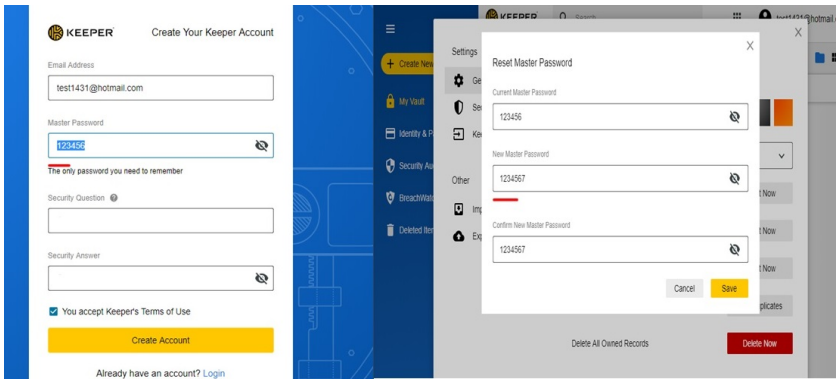

Figure A23. Keeper has a very weak policy for master passwords (the security question and answer are hidden in the left image.)

There is no random password generator in the browser extension (Keeper): This is a usability issue in Keeper as its browser extension does not have a random password generator like LastPass and Dashlane. The random generator is embedded in the password section in the application/webpage, so it is not separate. Recommendation: Keeper needs to put a random password generator in the browser extension so it can be accessed easily by users (severity: 3-Minor).

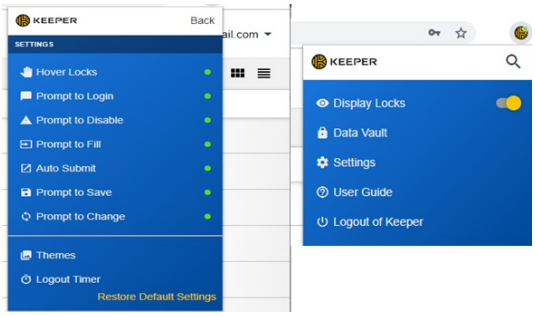

Figure A24. Keeper does not have a random password generator in the browser extension.

In the free version, users can only use an application, they cannot use a browser extension or webpage (Keeper): This is an issue for normal users who do not have a membership because they can only use the Keeper application on one device, and they cannot use the browser extension or log in to the webpage of Keeper. So, users cannot benefit from the autofill function if they do not subscribe. Recommendation: Keeper should allow its users to use the browser extension and webpage for free on their device, as well as allowing them to use an extra device for free (severity: 3-Minor).

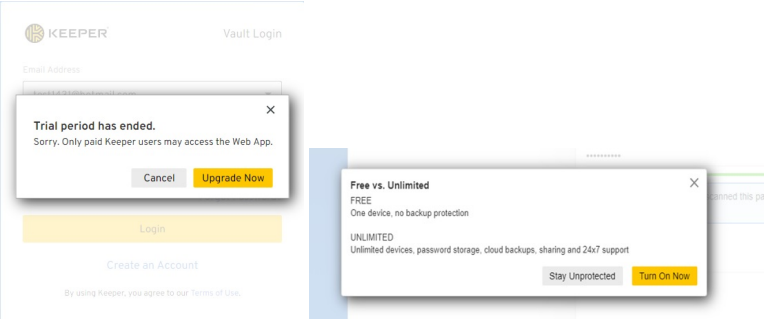

Figure A25. Webpage cannot be used on another device for free.

Old passwords are still stored in password managers: We found that old passwords that we had changed during the evaluation of LastPass and Dashlane were still stored and not permanently deleted, which raises a concern about users' data and trust and transparency issues with password managers.

Figure A26. Old passwords stored in LastPass.

References

1. Bonneau, J.; Herley, C.; Van Oorschot, P.C.; Stajano, F. Passwords and the evolution of imperfect authentication. *Commun. ACM* **2015**, *58*, 78–87. [CrossRef]
2. Haque, S.T.; Wright, M.; Scielzo, S. A study of user password strategy for multiple accounts. In Proceedings of the Third ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 18–20 February 2013; pp. 173–176.
3. Zhao, R.; Yue, C. All your browser-saved passwords could belong to us: A security analysis and a cloud-based new design. In Proceedings of the Third ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 18–20 February 2013; pp. 333–340.
4. Li, Y.; Wang, H.; Sun, K. A study of personal information in human-chosen passwords and its security implications. In Proceedings of the 35th IEEE International Conference on Computer Communications (INFOCOM 2016), San Francisco, CA, USA, 10–15 April 2016; pp. 1–9.
5. Florencio, D.; Herley, C.; Van Oorschot, P.C. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, USA, 20–22 August 2014; pp. 575–590.
6. Habib, H.; Naeini, P.E.; Devlin, S.; Oates, M.; Swoopes, C.; Bauer, L.; Christin, N.; Cranor, L.F. User behaviors and attitudes under password expiration policies. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, MD, USA, 12–14 August 2018; pp. 13–30.
7. Ion, I.; Reeder, R.; Consolvo, S. No one can hack my mind: Comparing Expert and Non-Expert Security Practices. In Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), Ottawa, ON, Canada, 22–24 July 2015; pp. 327–346.
8. Fagan, M.; Khan, M.M.H. Why do they do what they do? A study of what motivates users to (not) follow computer security advice. In Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO, USA, 22–24 June 2016; pp. 59–75.

9. Fagan, M.; Albayram, Y.; Khan, M.M.H.; Buck, R. An investigation into users' considerations towards using password managers. *Hum.-Centric Comput. Inf. Sci.* **2017**, *7*, 12. [CrossRef]
10. Chiasson, S.; van Oorschot, P.C.; Biddle, R. A Usability Study and Critique of Two Password Managers. *Usenix Secur. Symp.* **2006**, *15*, 1–16.
11. Stobert, E.; Biddle, R. The password life cycle. *Acm Trans. Priv. Secur.* **2018**, *21*, 13. [CrossRef]
12. Stobert, E.; Biddle, R. A Password Manager that Doesn't Remember Passwords. In Proceedings of the 2014 New Security Paradigms Workshop, Victoria, BC, Canada, 15–18 September 2014; pp. 39–52.
13. McCarney, D.; Barrera, D.; Clark, J.; Chiasson, S.; van Oorschot, P.C. Tapas: Design, implementation, and usability evaluation of a password manager. In Proceedings of the 28th Annual Computer Security Applications Conference, Orlando, FL, USA, 3–7 December 2012; pp. 89–98.
14. Li, Y.; Wang, H.; Sun, K. BluePass: A Secure Hand-Free Password Manager. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Niagara Falls, ON, Canada, 22–25 October 2017; pp. 185–205.
15. Li, Z.; He, W.; Akhawe, D.; Song, D. The emperor's new password manager: Security analysis of web-based password managers. In Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, USA, 20–22 August 2014; pp. 465–479.
16. Seiler-Hwang, S.; Arias-Cabarcos, P.; Marín, A.; Almenares, F.; Díaz-Sánchez, D.; Becker, C. I don't see why I would ever want to use it Analyzing the Usability of Popular Smartphone Password Managers. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 1937–1953.
17. Alkaldi, N.; Renaud, K. Why do People Adopt, or Reject, Smartphone Password Managers. Available online: http://eprints.gla.ac.uk/120760/7/120760.pdf (accessed on 29 October 2020).
18. Stobert, E.; Biddle, R. Expert password management. In Proceedings of the International Conference on Passwords, Cambridge, UK, 7–9 December 2015; pp. 3–20.
19. Ciampa, M. A comparison of password feedback mechanisms and their impact on password entropy. *Inf. Manag. Comput. Secur.* **2013**, *21*, 344–359. [CrossRef]
20. Ur, B.; Bees, J.; Segreti, S.M.; Bauer, L.; Christin, N.; Cranor, L.F. Do Users' Perceptions of Password Security Match Reality? In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 7–12 May 2016; pp. 3748–3760.
21. Gao, X.; Yang, Y.; Liu, C.; Mitropoulos, C.; Lindqvist, J.; Oulasvirta, A. Forgetting of passwords: Ecological theory and data. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 221–238.
22. Lyastani, S.G.; Schilling, M.; Fahl, S.; Backes, M.; Bugiel, S. Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 203–220.
23. Wash, R.; Rader, E.; Berman, R.; Wellmer, Z. Understanding password choices: How frequently entered passwords are re-used across websites. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS), Denver, CO, USA, 22–24 June 2016; pp. 175–188.
24. Pearman, S.; Thomas, J.; Naeini, P.E.; Habib, H.; Bauer, L.; Christin, N.; Cranor, L.F.; Egelman, S.; Forget, A. Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 295–310.
25. Poornachandran, P.; Nithun, M.; Pal, S.; Ashok, A.; Ajayan, A. Password reuse behavior: How massive online data breaches impacts personal data in web. In Proceedings of the Innovations in Computer Science and Engineering, Hyderabad, India, 22–23 July 2016; pp. 199–210.
26. AlMaqbali, F.; Chris, J.M. AutoPass: An automatic password generator. In Proceedings of the 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 23–26 October 2017; pp. 1–6.
27. Arias-Cabarcos, P.; Marín, A.; Palacios, D.; Almenárez, F.; Díaz-Sánchez, D. Comparing Password Management Software: Toward Usable and Secure Enterprise Authentication. *IT Prof.* **2016**, *18*, 34–40. [CrossRef]
28. Chiasson, S.; Forget, A.; Stobert, E.; van Oorschot, P.C.; Biddle, R. Multiple password interference in text passwords and click-based graphical passwords. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009; pp. 500–511.

29. Komanduri, S.; Shay, R.; Kelley, P.G.; Mazurek, M.L.; Bauer, L.; Christin, N.; Cranor, L.F.; Egelman, S. Of passwords and people: Measuring the effect of password-composition policies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada, 7–12 May 2011; pp. 2595–2604.
30. Stobert, E.; Biddle, R. The password life cycle: User behaviour in managing passwords. In Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS 2014), Menlo Park, CA, USA, 9–11 July 2014; pp. 243–255.
31. Pearman, S.; Zhang, S.A.; Bauer, L.; Christin, N.; Cranor, L.F. Why people (don't) use password managers effectively. In Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA, USA, 11–13 August 2019; pp. 319–338.
32. Aurigemma, S.; Mattson, T.; Leonard, L. So Much Promise, so Little Use: What Is Stopping Home End-Users from Using Password Manager Applications. In Proceedings of the Innovative Behavioral Is Security and Privacy Research, Hilton Waikoloa Village, HI, USA, 4–7 January 2017.
33. Golla, M.; Dürmuth, M. On the accuracy of password strength meters. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 1567–1582.
34. Wong, E. Heuristic Evaluation: How to Conduct a Heuristic Evaluation. 2020. Available online: www.interaction-design.org/literature/article/heuristic-evaluation-how-to-conduct-a-heuristic-evaluation (accessed on 29 July 2020).
35. Nielsen, J. Enhancing the explanatory power of usability heuristics. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Boston, MA, USA, 24–28 April 1994; pp. 152–158.
36. Nielsen, J. 10 Usability Heuristics for User Interface Design. 1994. Available online: www.nngroup.com/articles/ten-usability-heuristics (accessed on 29 July 2020).
37. Pierotti, D. Xerox/Nielsen 13 Usability Heuristics. Available online: https://uxmanager.net/heuristics/xeroxnielsen-13-usability-heuristics (accessed on 29 July 2020).
38. Broida, R. This Is the Best Free Password Manager. 2020. Available online: www.cnet.com/news/this-is-the-best-free-password-manager/ (accessed on 29 July 2020).
39. Coppock, M. The Best Password Managers for 2020. 2020. Available online: https://www.digitaltrends.com/computing/best-password-managers/ (accessed on 29 July 2020).
40. Rubenking, N.J. The Best Password Managers for 2020. 2020. Available online: https://uk.pcmag.com/password-managers/4296/the-best-password-managers (accessed on 29 July 2020).
41. Ellis, C.; Turner, B. Best Password Managers in 2020: Free, and Paid Apps for Secure Password Lists. 2020. Available online: https://www.techradar.com/uk/best/password-manager (accessed on 29 July 2020).
42. Miles, M.B.; Huberman, A.M. *Qualitative Data Analysis: An Expanded Sourcebook*; Sage: Newbury Park, CA, USA, 1994.
43. Virzi, R.A. Refining the test phase of usability evaluation: How many subjects is enough? *Hum. Factors* **1992**, *34*, 457–468. [CrossRef]
44. Faulkner, L. Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. *Behav. Res. Methods Instrum. Comput.* **2003**, *35*, 379–383. [CrossRef] [PubMed]
45. Hachman, M. Google Chrome's New Password Manager Makes Securing Chrome Even More Important. 2018. Available online: www.pcworld.com/article/3303596/google-chrome-new-password-manager.html (accessed on 29 July 2020).
46. Alkaldi, N.; Renaud, K. Encouraging password manager adoption by meeting adopter self-determination needs. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Grand Wailea, HI, USA, 8–11 January 2019.