

Building Trust around Password Managers

*A thesis submitted in partial fulfilment of the requirement for the degree
of Doctor of Philosophy by*

Fahad Suliman Alodhyani



School of Computer Science and Informatics

Cardiff University

January 2022

Acknowledgements

I would like to express my gratitude to my first supervisor, Dr George Theodorakopoulos and to my former supervisor, Dr Philipp Reinecke for their support and guidance during my PhD journey. I would also like to thank Dr Alia Abdelmoty for her support. The completion of my PhD could not have been possible without them. I would like to extend my gratitude to all participants who took part in the studies.

Finally, I would like to say thank you to my parents, my family and my friends for being supportive and caring throughout the course of my PhD.

Abstract

Passwords are considered to be the first line of defence in protecting online accounts and data. However, there are problems when people handle their own passwords such as password reuse and difficulty to memorize. Password managers appear to be a promising solution to help people handle their own passwords, but there is a low adoption of password managers even though they are widely available. Therefore, the issues that cause people not to use password managers must be investigated and, more generally, what users think about password managers in terms of usability and trust, and the user interfaces of password managers.

In this thesis, I conducted the following three studies: (1) an evaluation of the user interface and usability of three password managers using Nielsen's heuristics; (2) a user study about the usability of and user trust in password managers; and (3) an online questionnaire about users and non-users of password managers. The findings show that usability is only a minor issue for non-users while lack of trust is the main reason for not using password managers. Users of password managers have trust issues and security concerns with password managers. Also, cloud password managers offer useful features but there is a need to improve specific aspects, such as computer jargon and difficulty in account recovery.

So, in order to enhance trust and bridge the gap between people and password managers, I built and implemented a multi-platform prototype, which can be accessible from all popular web browsers on different devices, to improve transparency and control in

password managers. I conducted two user studies to evaluate it and the results show that improving transparency in password managers leads to a better understanding of the system and enhances trust in password managers.

Contents

Acknowledgements	ii
Abstract	iii
Contents	v
List of Publications	xi
List of Figures	xii
List of Tables	xviii
1 Introduction	1
1.1 Introduction	1
1.2 Contributions	5
1.3 Hypotheses and Research Questions	6
1.3.1 Users and non-users' perception of password managers	6
1.3.2 Usability of password managers	7

1.3.3	The influence of an educational background when using password managers	7
1.3.4	The impact of improving transparency in password managers	8
1.4	Thesis Organization	8
1.5	Conclusion	10
2	Literature Review	11
2.1	Introduction	11
2.2	Human Attitude towards Passwords and Password Management	12
2.2.1	Personal Information in Passwords	13
2.2.2	Length of Passwords	13
2.2.3	Reusing Passwords	14
2.3	The Effect of Security Education on Password Management	16
2.4	Proposed Solutions for Password Management	18
2.4.1	Password Policies	18
2.4.2	Password Strength Meters (PSM)	19
2.4.3	Single Sign-On (SSO)	20
2.4.4	Two-Factor Authentication (2FA)	21
2.5	Password Managers (PM)	21
2.5.1	Benefits of Password Managers	22
2.5.2	Problems with Password Managers	22

2.5.3	Solutions for Password Managers	25
2.5.4	Technology Adoption Life Cycle	28
2.5.5	Call for Further Investigation	30
2.6	Conclusion	31
3	Evaluation of Password Managers Using Nielsen's 10 Principles	32
3.1	Introduction	32
3.2	Methodology	34
3.3	Result	36
3.3.1	Positive Aspects of the Three Cloud Password Managers	39
3.3.2	Negative Aspects of the Three Cloud Password Managers	43
3.4	Discussion	61
3.5	Conclusion	63
4	User Study about Usability and Trust of Password Managers	65
4.1	Introduction	65
4.2	Methodology	66
4.3	Result	71
4.3.1	Usability Test	72
4.3.2	Interview Section	80
4.4	Discussion	90

4.5	Conclusion	92
5	Questionnaire Study about Users and Non-users of Password Managers	93
5.1	Introduction	93
5.2	Methodology	95
5.3	Result	96
5.3.1	Non-users of Password Managers	100
5.3.2	Users of Password Managers	108
5.4	Discussion	122
5.5	Conclusion	124
6	A User Study about Improving Transparency in Password Managers	125
6.1	Introduction	125
6.1.1	The Role of Transparency	127
6.2	Design a Prototype of Password Managers	128
6.3	Methodology	132
6.4	Result	133
6.4.1	Comparing Non-transparent and Transparent Managers	135
6.4.2	Usability of Transparent Password Manager	142
6.5	Discussion	147
6.6	Conclusion	148

7	An Extended User Study about Improving Transparency in Password Managers	149
7.1	Introduction	149
7.2	Design a Prototype of Password Managers	150
7.3	Methodology	151
7.4	Result	151
7.4.1	Comparing Program A and Program B	153
7.4.2	Features of Program B	158
7.4.3	Usability of Program B	160
7.5	Discussion	163
7.5.1	Recommendations for Improving Password Managers	165
7.6	Conclusion	166
8	Discussion and Conclusion	167
8.1	Summary	167
8.2	Discussion	168
8.3	Research Findings and Contributions	174
8.4	Future Work	176
8.5	Conclusion	176
	Bibliography	177

A Appendix	198
A.1 Chapter 4 (Questions for User Study)	198
A.2 Chapter 5 (Questions for Online Questionnaire)	203
A.3 Chapter 6 (Questions for Improving Transparency in Password Managers)	207
A.4 Chapter 7 (Questions for Improving Transparency in Password Managers “extended study”)	211
A.5 More Comments and Tables for Chapter 4, 5, 6, 7	215
A.6 More Screenshots for two Programs (Chapter 6 / 7)	220

List of Publications

- Alodhyani, F.; Theodorakopoulos, G.; Reinecke, P. Password Managers—It’s All about Trust and Transparency. *Future Internet* 2020, 12, 189.
<https://doi.org/10.3390/fi12110189>

List of Figures

1.1	Thesis organization.	9
3.1	Remove username from LastPass. Remove password from Dashlane without undo function for this action. Remove username from Keeper without undo function, and no undo for deleting all records as it is a paid feature (personal email is hidden).	46
3.2	LastPass does not prevent users from storing wrong data, for example, incorrect URL, alphabetic instead of numerical characters.	47
3.3	Keeper does not prevent users from storing wrong data, for example, incorrect URL and phone no (part of phone number is hidden).	47
3.4	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.	48
3.5	LastPass does not prevent users from storing the same account twice (with different passwords). The same Twitter account can appear twice on LastPass vault. Also, in Twitter, the autofill login form shows the account twice (from 2020).	49

3.6	Dashlane does not prevent users from storing different passwords for the same account.	49
3.7	Keeper does not prevent users from storing different passwords for the same LastPass account (personal emails are hidden for other accounts). A screenshot from 2020 with a better quality.	50
3.8	Data entry forms in LastPass, Dashlane and Keeper, which do not have asterisks. (Part of password in Dashlane is hidden).	51
3.9	Computer jargon used in Dashlane (menu of Dashlane app)	51
3.10	LastPass uses different words for the same action, change master password and set master password (no consistency).	52
3.11	Computer jargon (account settings in LastPass).	52
3.12	Computer jargon used in Keeper (part of phone number is hidden).	52
3.13	Colour of LastPass account settings. (Personal email and date are hidden).	53
3.14	LastPass allows users to create a weak master password that does not match its policy.	53
3.15	Auto-change password does not work in LastPass for Twitter. Also, it does not support all websites, for example, Hotmail. (Personal email is hidden).	54
3.16	Random password generator for LastPass.	55
3.17	Very strict as users must use the same device and browser that was used before to recover and access LastPass account.	55

3.18	Required authentication such as SMS code, and authentication app such as LastPass authenticator app (if the app of Multifactor authentication is enabled).	56
3.19	Colour of application and webpage of Dashlane.	56
3.20	Users of Dashlane can create a master password using their email address.	57
3.21	Changing the master password while synchronization is disabled causes a loss of data stored on other devices.	57
3.22	Recovering Dashlane account requires business team membership (not free).	58
3.23	The application has all the features and functions, while the webpage does not.	58
3.24	Keeper has a very weak policy for master passwords (the security question and answer are hidden in the left image.)	59
3.25	Keeper does not have a random password generator in the browser extension (an icon next to Keeper extension is hidden).	60
3.26	In Keeper, the webpage cannot be used on another device for free.	60
3.27	Old passwords stored in LastPass.	61
4.1	Answers by 16 users and 14 non-users for (Yes/No) questions about password managers and the similarities between the two groups.	83
6.1	Homepage of the website (prototype) which shows information and instructions about the study. A screenshot from a desktop (left) and a smartphone (right).	129
6.2	Main page of a non-transparent PM. It shows a stored account, website name/URL, username and plain password.	129

-
- 6.3 Main page of a transparent PM. It shows a stored account, website name/URL, username, encrypted password and time of storing it. Also, there is an image embedded on the top right explaining how the system works. 129
- 6.4 Details of a non-transparent manager page (left), it only shows a username, plain password and website name/URL. Details page of a transparent manager (right), as participants can see an encrypted password, encryption key, time of storing, location and synchronization. The password can be decrypted using the same key and an image is embedded at the top which is about how the system works. Also, there is an external link to check the strength of password provided on the details page. . . . 130
- 6.5 The text box is about a random password generator and an advice of using one. Also, a website link is embedded which explains about password generator. 130
- 6.6 Adding an account in a non-transparent PM (left), there are only forms for username, password and website name/URL. Password generator buttons are in colour. Adding an account page in a transparent PM (Right), participants can generate an encryption key, know its length and the algorithm used. They can choose a place to store each password and view the location on Google maps (simulated). They can generate a random password using a generator which shows the strength of password in words and colours. They can allow or prevent password synchronization for each password (simulated). 131
- 6.7 System Usability Scale (SUS) scores. The figure is taken from an article for Bangor *et al.* [135], An empirical evaluation of the system usability scale. 143
- 7.1 Homepage of the website which shows information and instructions. . . . 150

-
- 7.2 Main page of program A. It shows a website name/URL, username and a password as asterisks (it only shows the password when a user puts the cursor on the eye icon). 151
- A.1 Adding an account in non-transparent/program A, there are only forms for username, password and website name/URL. Password generator buttons are in colour. When saving a new password, the program informs user that the password has been stored. 220
- A.2 Details page of program A, it only shows a username, password (asterisk) and website name/URL. The second screenshot shows the password when a user puts the cursor on the eye icon. 221
- A.3 Main page of program A which shows a stored account. The page shows website name/URL, username and password as asterisk. The second screenshot shows the password when a user puts the cursor on the eye icon. . . . 221
- A.4 Adding an account page in transparent/program B. There is a button to generate an encryption key to encrypt the password, different options to choose from to store each password and view the location on Google maps. A random password can be generated using a random password generator which shows the strength of password in words and colours. Finally, password synchronization can be allowed or prevented. 222
- A.5 Adding an account page in transparent/program B. The screenshot on the left shows a button that generates an encryption key when a user puts the cursor on. The screenshot on the right shows the generated key (the button disappears once it is clicked). 223
- A.6 Adding an account page in transparent/program B. The random password generator generates different types of passwords such as very weak and strong. 223

-
- A.7 Adding an account page in transparent/program B. The program offers different storage locations to store passwords, e.g., Headquarters. It also offers an option where passwords can be synchronized across devices or prevented (all simulated). 224
- A.8 Adding an account page in transparent/program B. When a user puts the cursor on the text box, it shows an explanation about the storage location. 224
- A.9 Adding an account page in transparent/program B. When the button “Encrypt and Save” is clicked, the new password will be encrypted and saved. The link (URL) of the program is hidden in the screenshot. 225
- A.10 Main page of transparent/program B which shows a stored account. The page shows website name/URL, username, encrypted password and time of storing it. 225
- A.11 Details page of transparent/program B. The page shows the username, encrypted password, encryption key, time of storing, location and synchronization. The password can be decrypted by clicking on the button (second screenshot). Also, there is an external link to check the strength of stored password. 226

List of Tables

2.1	A summary of the effect of education on password behaviour.	17
2.2	A summary of factors that affect password behaviour.	25
2.3	A summary of factors that affect the adoption of password managers. . . .	25
2.4	A summary of the proposed password managers by researchers (section 2.5.3).	27
3.1	Nielsen’s 10 principles and definition [28], [29]	35
3.2	A summary of popular password managers in 2019.	37
3.3	A summary of other popular password managers in 2022 [115].	38
3.4	Positive aspects and Nielsen’s principles applied to three password managers.	39
3.5	Problems, violations of Nielsen’s principles and severity ratings for LastPass, Dashlane and Keeper.	44
3.6	A summary of the important problems that affect password managers. . . .	61
4.1	Definition of three factors used to compare between users and non-users . .	69

4.2	Number of users and non-users of password managers.	71
4.3	11 Statements were answered by 30 participants about using LastPass and specific functions.	73
4.4	The mean (average) and median, Mann Whitney U value and p-value of each usability statement for 16 users and 14 non-users (ease of use). For p-values, exact significance is displayed [2*(1-tailed sig.)].	75
4.5	Three questions were answered by 30 participants about their satisfaction with using LastPass.	76
4.6	The mean (average) and median, Mann Whitney U value and p-value of each question for 16 users and 14 non-users (satisfaction). For p-values, exact significance is displayed [2*(1-tailed sig.)].	77
4.7	Answers sample for the question “Most liked?”.	78
4.8	Comments sample about LastPass password manager.	79
4.9	Overall answers by 30 participants for (Yes/No) about password managers.	82
4.10	Comments sample for the question “Trust the vendor of a password manager to store all passwords?”.	85
4.11	Comments sample for the question “Trust password managers to delete password permanently?”.	86
4.12	Comments sample for the question “Have you ever used a random generator?”.	88
5.1	Number of experts and non-experts in this study.	96
5.2	Number of online accounts for 128 experts and 119 non-experts.	97
5.3	Number of passwords for 128 experts and 119 non-experts.	98

5.4	Number of users and non-users, including experts and non-experts.	99
5.5	Number of passwords for 113 users and 134 non-users.	100
5.6	Number of accounts for 113 users and 134 non-users.	100
5.7	Number of times each reason was selected by 134 participants (66 experts and 68 non-experts), which also means these reasons were not selected by the remaining participants. It shows the overall time and percentage of reasons selected by both groups. Note: numbers do not add up to 100% as participants could choose more than one reason.	102
5.8	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.	104
5.9	Every three reasons from Table 5.8 were grouped in a category. McNemar test was used to see if there was any significant difference between these categories.	105
5.10	Comparing between 4 categories that were selected/not selected by 134 non-users. McNemar test was used to find the significant difference between the categories.	106
5.11	Types of password managers used by 113 users (62 experts, 51 non-experts).	109
5.12	62 experts and 51 non-experts (113 users) who store all or some passwords.	109
5.13	62 experts and 51 non-experts (113 users) who use a password generator.	110

5.14	Answers sample for “Why are you using a password manager?”. Frequencies of codes being applied to participants’ reasons for using password managers. Please note that numbers add up to 100%. Participants could have one or more reasons in one answer.	112
5.15	Analyzing 5 different password managers (number of users for each program).	113
5.16	10 Usability statements were answered by users of password managers. . .	115
5.17	12 Statements were answered by 113 users about password managers. . .	118
5.18	Comparing 62 experts and 51 non-experts regarding using password managers. The mean (average) and median, Mann Whitney U and p-value of each statement.	121
6.1	Number of online passwords for 132 participants.	134
6.2	Number of experts and non-experts.	134
6.3	Type of devices used in this study	134
6.4	Number of users and non-users of password managers.	135
6.5	I know where my online passwords are stored.	135
6.6	I fully understand how my passwords are processed.	136
6.7	I understand how it works.	136
6.8	I understand how it generates the encryption key.	137
6.9	I understand the benefit of a random password generator.	137
6.10	I trust it to store all my online passwords.	138

6.11	I trust it to delete my password from its database permanently after I have deleted it from my account.	138
6.12	I trust it to generate a strong key to encrypt my password.	139
6.13	I feel that I have control of my passwords when I store them.	139
6.14	Password is stored securely in it.	140
6.15	I trust it for not synchronizing my passwords over different devices (e.g., computers, smartphones) without my permission.	140
6.16	Comparing between non-transparent (Non) and transparent (Tra) password managers using a Wilcoxon Signed-Ranks test. The table shows the mean (average) and median, Z score and p-value of each statement.	141
6.17	System Usability Scale (SUS) Score.	143
6.18	SUS questions were answered by 132 participants about transparent manager.	144
6.19	Comments sample about the things they like most in a transparent manager.	145
6.20	Comments sample about the things they dislike most in a transparent manager.	146
7.1	Number of experts and non-experts.	152
7.2	Type of devices used in this study	152
7.3	Number of users and non-users of password managers.	152
7.4	Number of online passwords for 68 participants.	153
7.5	I know where my online passwords are stored.	153
7.6	I fully understand how my passwords are processed.	153

7.7	I understand how it works.	154
7.8	I understand how it generates the encryption key.	154
7.9	I understand the benefit of a random password generator.	154
7.10	I trust it to store all my online passwords.	155
7.11	I trust it to delete my password from its database permanently after I have deleted it from my account.	155
7.12	I trust it to generate a strong key to encrypt my password.	155
7.13	I feel that I have control of my passwords when I store them.	156
7.14	Password is stored securely in it.	156
7.15	I trust it to not synchronize my passwords over different devices (e.g., computers, smartphones) without my permission.	157
7.16	Comparing between program A and program B using a Wilcoxon Signed- Ranks test. The table shows the mean (average) and median, Z score and p-value of each statement.	158
7.17	51 Participants answered 9 questions about the importance of each fea- ture/ factor of program B. The range is from not important at all to very important.	159
7.18	Comments by participants about preferring program A over program B. . .	160
7.19	System Usability Scale (SUS) Score.	160
7.20	SUS questions were answered by 68 participants about program B. . . .	161
7.21	Comments sample about the things they like most in program B.	162
7.22	Comments sample about the things they dislike most in program B. . . .	163

A.1	For the question “How would you save master password?”	215
A.2	For the question “Install a browser extension on a shared computer?” . . .	215
A.3	For the question “Checked the strength of master password?”	215
A.4	For the question “What will happen if master password is compromised?”	216
A.5	For the question “What did you like the least?”	216
A.6	For the question “Where would you expect to find a random generator?” .	216
A.7	For the question “What would you do if password manager fails to work?”	217
A.8	For the question “Why are you using a password manager?”	217
A.9	For the question “Add emergency contact to recover the account?”	217
A.10	For the question “Let a password manager store bank and passport details?”	218
A.11	For the question “Reuse password in multiple accounts?”	218
A.12	Answers sample for not using a password generator (Chapter 5). Frequen- cies of codes being applied to participants’ reasons for not using random generator. The numbers add up to 100%. Participant’s answer could have different reasons.	218
A.13	Comparing between non-transparent and transparent managers (Chapter 6). Using a Wilcoxon Signed-Ranks test to find mean ranks (negative and positive).	219
A.14	Comparing between program A and program B (Chapter 7). Using a Wilcoxon Signed-Ranks test to find mean ranks (negative and positive). .	219

Chapter 1

Introduction

1.1 Introduction

We live in an era where technology has become an essential part in our daily life. People rely on technology to do shopping, pay bills, transfer money, and use social media to communicate with each other. The rapid increase in the reliance on technology has created another privacy issue regarding people's personal information as most online websites only use text-password (string of characters) to protect online accounts.

The reason for using text-password is related to its cost effectiveness, simple and easy to use. Password is considered to be the most popular authentication method due to its cost effectiveness and its simplicity [1]. Bonneau *et al.* said that passwords have dominated for 50 years for authentication in spite of consensus by researchers that we need something more user-friendly and secure [2]. The fact is that people are still relying on passwords, even though there were speculations in the past about eliminating passwords in the future.

In 2004, Bill Gates said that people are going to rely less on passwords over time [3], while IBM (2011) stated that "You will never need a password again" [4]. However, because a trustworthy replacement is unavailable, people are still relying on password for authentication and will keep relying on them in the future [5]. Also, single password remains widely used for authentication [6]. So, there are people who stated that passwords would be eliminated in the future, while others do not think it is possible.

If truth be told, it is very easy to use passwords, but the main issue is that people create weak passwords, reuse the same password in multiple accounts, write them down in an insecure place and include personal information within the password. Because of human memory limitations, users find it difficult to memorise strong, long, and random passwords that are hard to crack [7]. A leaked password dataset from a Chinese website was analyzed and it was found that passwords contained personal information such as names and birthdates [8]. Therefore, we can see that thousands of passwords have been compromised because people select bad passwords as it is difficult to memorize and manage strong passwords.

In response to these insecure practices, a number of tools have been developed in order to help people handle their own passwords. A password policy is a set of requirements that were designed to help users create a strong password, such as add upper-case and special characters. To create a strong password, a password strength meter (PSM) was proposed which guides users to create a strong password as it shows the level of password if it is weak, average, or strong. Single sign-on (SSO) allows users to authenticate themselves in the first instance and after that they can access different applications with the same credentials, for example, a user can use their Gmail account/password to access YouTube and LinkedIn which decreases the need to create many passwords. However, these solutions have limitations that make it hard for people to create, remember and manage their own passwords properly. For example, users cope with password policy by modifying current passwords, password meters are inconsistent and sometimes provide misleading password strength, while SSO is only accepted by specific websites.

Another solution is a password manager that can generate a random password and store it in the database, so, the user only needs one password to remember which is called the master password. Password managers generate, encrypt and store passwords for a user, while the user is required to remember the master password and a username [9]. If a password manager is not used, reusing passwords and grouping accounts become the only manageable solution [10], [11]. Organizations should consider using password man-

agers with a built-in generator because people might not create and preserve passwords by themselves [12]. Actually, password managers can be a promising solution because it is widely available, it generates a unique and strong password for each account which can mitigate weak passwords and password reuse, and also it can store multiple passwords without the need to memorize them.

Existing literature focuses mainly on passwords or on the technical and security side of password managers [7], [10], [13]–[22], but rarely on the usability of password managers and the human perspective of the tools. As password managers have been built for people to use, then the opinion of these people need to be investigated and explored to find a suitable solution. Therefore, the aim of this research is to focus mainly on password managers as well as the perspective of users and non-users, and to investigate about password managers in different aspects such as usability and trust.

Trust is defined as the hope and expectation that something is true as well as something is safe and reliable [23]. For example, a user trusts a password manager to store their passwords because they expect the system will manage their passwords safely. The definition of transparency is the quality of being done in an open way without secrets [24]. So, transparency is that a user can see what is happening in the other end, such as how passwords are processed. Regarding the meaning of adoption, it is the process of starting to use a new product or service [25]. Also, adoption is the act of embracing, accepting and starting to use something new such as idea and principle [26]. Regarding the definition of security, it is protecting information against being used wrongly or stolen [27], such as preventing passwords theft and passwords lost.

In the first step of the research, I investigated about the user interface and specific functions of three cloud password managers (LastPass, Dashlane and Keeper) using Nielsen's 10 principles [28], [29]. Nielsen's 10 principles are useful to evaluate the user interface design and usability of programs and identify problems in the programs and suggest solutions. The principles are also helpful to identify the positive aspects of the programs. So, the principles are useful to identify the good features of the password managers, and

identify the problems and issues in the user interface and usability. I found that the three password managers have consistent design and provide features such as storing passwords, fill in credentials and password generators. However, they have issues that exist which should be improved such as the weak policy of the master password, there is no undo function after saving new changes and the use of computer jargon.

I also focused on the human perspective of password managers by conducting a user study with 30 participants. The findings show that users and non-users of password managers found it easy to create an account, store and access passwords in a password manager and they were satisfied with the overall experience. However, the two groups have a lack of trust towards password managers as they do not trust it to store all passwords or delete them permanently from the database. Furthermore, many of them do not know where passwords are stored or how they are processed.

Moreover, I extended the study by conducting an online questionnaire with a larger group which was completed by 247 participants. The findings show that a lack of trust and transparency along with security concerns are the main issues for not using password managers, because non-users do not trust password managers to store passwords and they do not know where passwords are stored. For users, they found password managers easy to use and store passwords, but they have trust and transparency issues in regard to storing all passwords as well as security concerns. In the same study, I found significant difference in the number of passwords between experts (participants who have an educational background related to computer science or information security) and non-experts (participants with different educational background). However, there was no significant difference between experts and non-experts in adopting password managers.

Based on the findings from the three studies, I designed and implemented a solution (prototype) to improve transparency in password managers. The system allows users to choose a place to store passwords, generate an encryption key and allow/prevent password synchronization. I conducted two user studies to test the hypothesis; the first user study was completed by 132 participants and the extended study was completed by 68 partici-

pants. Quantitative data was evaluated descriptively and statistically, and qualitative data was evaluated using inductive coding. The findings show that improving transparency leads to a better understanding of the system and enhances trust in password managers.

1.2 Contributions

My research looks at the user interface and usability of three cloud-based password managers as well as the human perspective in the use and non-use of password managers in regard to four key aspects (usability, trust, transparency and security). I used different methodologies to understand the obstacles of the low adoption of password managers, understand the users' view of password managers and also compared between expert and non-expert participants in several areas such as the use and non-use of password managers. The findings of the studies helped to design a new solution to solve the problems.

List of contributions:

- In the evaluation of three cloud password managers using Nielsen's 10 principles (chapter 3), I found that cloud password managers provide good features for users to utilize such as; storing passwords, storing personal data, fill in credentials and password generators. However, they should improve issues such as computer jargon, recover account when a master password is forgotten and impose strong requirements for the master password.
- In the user study (chapter 4), users and non-users of password managers found it easy to store and access passwords in LastPass, and they liked saving passwords the most. However, the two groups have similar experience regarding password managers such as they did not know where passwords are stored or how passwords are processed. Also, non-users did not trust password managers to store all passwords or delete them permanently from the database.
- In the online questionnaire study (chapter 5), trust and transparency issues are the

reasons for not using password managers along with security concerns, for example, non-users do not trust password managers to store passwords. Regarding users of password managers, they found it easy to use, access and store passwords, but they have trust issues and security concerns. Also, education does not help to mitigate password reuse problem.

- Finally, I designed a prototype which improves transparency in password managers (chapter 6 and 7). It allows users to generate a key, encrypt passwords, choose a location to store passwords and show details of stored passwords. The results of the two user studies show that making the system transparent to people can help enhance trust in password managers and lead to a better understanding of the system.

1.3 Hypotheses and Research Questions

In this section, I state the hypotheses for this thesis and below each hypothesis, there is a list of research questions that explains the hypotheses further and in more details.

1.3.1 Users and non-users' perception of password managers

Hypothesis 1: Users of password managers have trust, transparency and security concerns, while non-users do not use password managers due to trust and transparency issues.

- (1) Are there any similarities in the reporting experience between users and non-users of password managers in terms of trust, transparency and knowledge regarding password managers?
- (2) Do users of password managers have trust issues and security concerns towards password managers?
- (3) What are the reasons behind the low adoption rate of password managers among non-users?

1.3.2 Usability of password managers

Hypothesis 2A: Password managers are easy to use for users and the design of their user interfaces satisfies Nielsen's principles.

Hypothesis 2B: Users and non-users of password managers are equally satisfied with the usability of LastPass cloud password manager.

- (1) Do the usability and user interface design of current cloud-based password managers satisfy Nielsen's 10 principles?
- (2) Do users and non-users of password managers have similar experience in terms of ease of use and satisfaction when they use LastPass cloud password manager?
- (3) Are current password managers easy to use for users of password managers?

1.3.3 The influence of an educational background when using password managers

Hypothesis 3: Having an educational background related to computer science or information security increases the understanding of the benefit of password managers, so it plays a significant role in the adoption rate for password managers. Also, education plays a significant part in the perception of experts and non-experts when they use (or do not use) password managers as well as mitigates password reuse.

- (1) Does an education in computer science or information security play a significant role in adopting password managers and mitigating password reuse?
- (2) Are there any differences between expert and non-expert users of password managers in terms of their perception of password managers in different aspects such as transparency and trust?

- (3) Are there any differences between expert and non-expert non-users of password managers in terms of their perception of password managers in different aspects such as security and trust?

1.3.4 The impact of improving transparency in password managers

Hypothesis 4A: Improving transparency in password managers will lead to a better understanding of the system.

Hypothesis 4B: Improving transparency in password managers will enhance the trust in password managers.

1.4 Thesis Organization

The rest of the thesis is organized as follows:

- **Chapter 2:** Literature review on human attitude towards passwords and proposed solutions for password management.
- **Chapter 3:** Evaluation of user interface and usability of cloud password managers using Nielsen's 10 principles.
- **Chapter 4:** User study about the usability and trust of password managers.
- **Chapter 5:** Online questionnaire about users and non-users of password managers.
- **Chapter 6:** User study about improving transparency in password managers.
- **Chapter 7:** An extended user study about improving transparency in password managers.
- **Chapter 8:** Discussion and Conclusion.

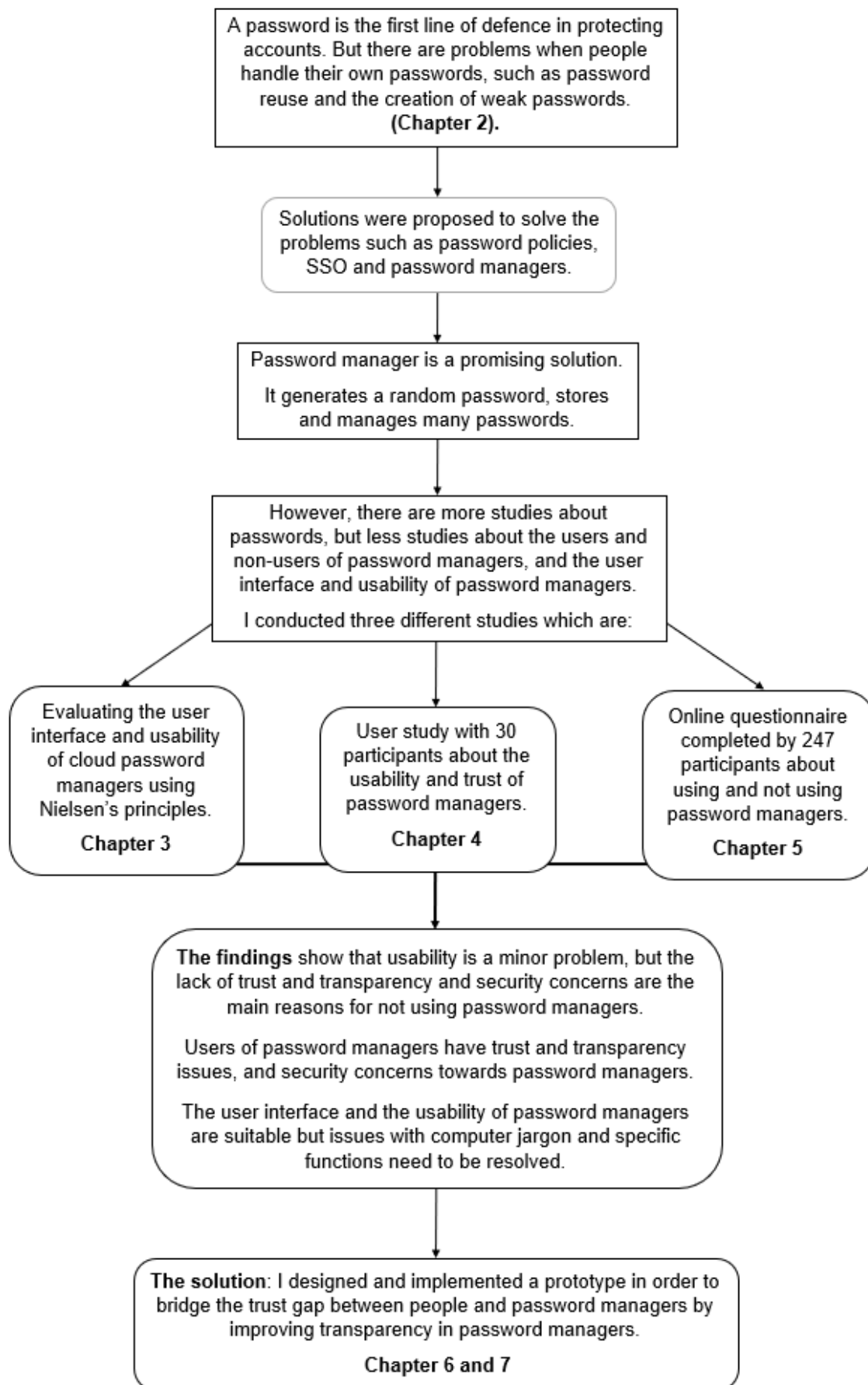


Figure 1.1: Thesis organization.

1.5 Conclusion

The next chapter investigates the current problems surrounding passwords and what have been done in the last few years to solve these problems. I reported a variety of studies about important topics in passwords and other tools; starting with the human attitude towards passwords and password management, and explored it with current solutions such as password policies and password managers.

Chapter 2

Literature Review

2.1 Introduction

This chapter investigates how people handle their own passwords, the problems they make and the solutions that have been proposed to solve these problems, for example, password policies and password managers. In fact, passwords have been widely used for many years because it is very simple and easy. However, there are problems associated with passwords which put people's accounts and privacy at risk.

In the early 1980s, Lamport identified three problems that an intruder can exploit to obtain user's passwords. The first problem when the intruder gains access into the information inside the system, while the second problem is intercepting the user's communication with the system. The third problem is the user's inadvertent disclosure of their own password [30]. So, the third problem became one of the main concerns because users do not manage their own passwords safely and properly.

The problems are that people create weak passwords, write passwords down in an insecure place, reuse passwords in multiple accounts and include personal details in their passwords. User behaviour facilitated the security breaches in many reported cases [31]. Stobert and Biddle said that users do not want to trust other people to remember their passwords, meanwhile they do not want to remember their own passwords which is a complex issue [14]. Early in 2021, more than 3 billion emails and passwords from websites such as LinkedIn and Netflix were leaked online and the possible impact is unprecedented

because of reusing passwords in multiple accounts [32].

As a matter of fact, even though these problems were identified, we cannot stop using password because we need it. Passwords are still widely used and it seems that it cannot be replaced for many years to come. Zimmermann and Gerber conducted a lab study and investigated user perceptions of twelve different authentication schemes such as password, fingerprint, photo TAN and associative questions. They found that a password has the highest score in regard to usability, preference and intention to use because it is easy to use, the speed is high and perceived security [33]. Therefore, solutions have to be devised in order to help people create strong passwords and manage them safely to protect their personal data.

2.2 Human Attitude towards Passwords and Password Management

Bonneau *et al.* said “In addition to being regarded as the weak link in password systems, users are also typically the most difficult component to model” [2]. Many users have some algorithms for developing passwords that are secure, while other algorithms lead to an easy to guess password [34]. In a study about improving password memorability, users were shown to remember the new password better if they are asked to verify it three times when they create a new account [35]. In another study, it was suggested that the poor recall of password is not related to a poor memory as there is no relationship between recalling correct password and memory performance, thus, there could be other factors involved in poor recall of password [36].

2.2.1 Personal Information in Passwords

A data-set of a large bank in the Middle East was analyzed and cracking tools like John the Ripper was used. The result shows that passwords are biased by location, culture and included names, birth dates, and phone numbers within passwords [37]. In a study about password behaviours in culture and gender, it was found that more participants from China use family names in their passwords compared to participants from Turkey and United Kingdom [38].

The result of another study shows that participants created their initial passwords by applying techniques like using an English word, name, and adding numbers or symbols to the beginning or the end of a name or word [12]. In a study about socio-cultural factors in how users create their own passwords, the data-sets of specific countries show local social influences, for example, a football club in United Kingdom, the name Nicholas in France and Giuseppe in Italy [39].

Moreover, Gao *et al.* applied an ecological theory in the study and found that most participants were capable to remember their passwords, but they chose to use saving feature or write passwords down to avoid forgetting them [40]. They also stated that the major strategies applied by participants to memorize passwords are by including names and familiar items, while other participants memorize own passwords based on keyboard layout or by recalling passwords more frequently to remember them [40].

2.2.2 Length of Passwords

Security researchers analyzed 32 million passwords that were posted on the internet, they found 12% of passwords were 9 characters in length or longer, while 60% of users chose their passwords from a limited set of characters and 30% of passwords were only 5 or 6 in length [41]. Additionally, 185.643 plaintext passwords from university students in Europe were analyzed [42], the result shows that the average length of characters is 6,7.

More to this point, over six million passwords were measured regarding their length and selection, the finding is that the average length of passwords is 9.46 characters, while over 70% of passwords include symbols such as “@” and “!” [43]. Likewise, the average length of passwords from a leaked data-set from a Chinese website is 8.44 [8]. In a study about culture and gender differences, participants from United Kingdom have the longest of the shortest passwords (7.6 characters) compared to participants from Turkey (6.5 characters) and China (5.8 characters) [38].

2.2.3 Reusing Passwords

If users reuse a password in multiple accounts, a hacker could gain access to other accounts once they gain access to one account [44]. The attacker could gain access to several accounts if they discover one reused password [14]. Also, participants know the reuse of passwords is entirely insecure but memorable [45], while 91% of participants reused at least one of their passwords for multiple accounts [40]. Researchers found that people reuse password in multiple websites because the number of websites is larger than the number of passwords [46].

Pearman *et al.* analyzed data which was collected by Security Behaviour Observatory; they found that most participants reused passwords in multiple accounts, while an average participant used 9.88 unique passwords for 26.34 different accounts [47]. The finding also suggested that users cope with large number of passwords by reusing the same password or part of it, as the average participant reused of exact passwords or partially is 79% [47]. Another study about passwords found that 51% of participants reuse passwords in personal and business accounts, 69% admit sharing passwords with colleagues and 57% do not change password behaviour to prevent such an attack [48].

Furthermore, many participants misunderstood advice about using symbols and digits in password, because they expected weak password would become secure when adding digits and symbols [34]. Users reuse and share password and they tend to adjust an old

password to create a new one [49], while widespread password reuse was found as 63.8% of participants use passwords elsewhere and they knowingly reuse weak passwords [50].

Users choose a complex password which they use it frequently in one website and reuse it in other websites [46]. Poornachandran *et al.* collected data from websites such as Twitter and tried valid username/password combination on Facebook, Gmail and Hotmail, in which they found 33% password reuse behaviour on Facebook, 15% password reuse on Gmail and 26% on Hotmail [51]. They found that 59% of participants reuse passwords in multiple websites due to the difficulty remembering a large complex password, so reusing strong password or similar password in many accounts make it vulnerable [51].

Additionally, a high percentage (75%) of participants reuse passwords as the vast majority did it because it is easy to remember and because of speed, while 62% did not reuse passwords for online banking or websites that saved credit card (43%) [13]. Also, 81% created variations of password to use in different websites, while 61% said they never or rarely wrote their passwords down [13]. 85% of passwords that used on high-value accounts (financial websites) were used in different websites categories, while passwords used on job and shopping websites are likely to be reused in many accounts [47].

It was found that 70% of participants have passwords exclusively used for important accounts, which shows that participants have groups of accounts and manage the important group differently [52]. Linking password lifetime to strength at the stage of creating passwords, can encourage users to choose stronger passwords, as well as users will change passwords when they receive password expiry warning [53]. Thus, to nudge users away from creating weak passwords is to increase security motivation such as adding payment card [54].

2.3 The Effect of Security Education on Password Management

Having education in information security or working in an information security field could help mitigate the problem with passwords such as password reuse. Ion *et al.* compared between security experts who have at least 5 years of experience studying or working in computer security field and non-experts [55]. They found that experts have more unique passwords than non-experts, experts reuse less passwords than non-experts, they write less passwords down compared to non-experts and they use password managers more than non-experts. In contrast, non-experts have stronger passwords than experts, they change passwords more frequently and they have a higher percentage in remembering passwords compared to experts. The researchers found that non-experts have lack of understanding of the security benefits of password managers, while the poor usability of password managers might stall the adoption among them [55].

Similarly, Stobert and Biddle conducted an interview study with participants who were not studying computer science or computer security [56]. The study shows that 96% of participants reuse passwords, 81% saved passwords in the saved feature in browsers or apple keychain, and 78% write down at least one of their passwords. They found that none of participants use dedicated password manager which indicates that most participants are not aware of prominent password manager [56]. Also, they conducted another interview study with experts from community of industry security and information security group where the majority have a degree in computer security [57]. They found that the majority of participants reuse their own passwords on at least some of their accounts, but they have a careful strategy as they do not reuse all passwords. Also, 9 participants write passwords down, several participants relied on password managers to generate passwords, while 12 participants use password managers and half of them use dedicated password managers [57]. The main difference between experts and non-experts is that non-experts almost did not discuss any security problems [13].

Additionally, in a study with 100 participants from 3 groups (IT professionals, students who are not enrolled in an information technology security program, and a general group) [58], Alomari and Thorpe found that 100% of students reuse password compared to 82% of general group and 77% of IT professionals. All groups include names when selecting passwords and students have the most names, while IT professionals are the least to record passwords. IT professionals are more likely to use random and stronger passwords and reuse fewer passwords. The IT professionals employ some secure behaviours and have confidence in computer security knowledge [58]. However, there are no differences between the three groups in sharing passwords. Surprisingly, 74% of IT professionals used a variation of old passwords to create new passwords compared to students (61%) and the general group (58%).

It was stated that educating users is a major initiative to enhance credentials security, and there is a need to educate users about potential solutions which are password managers and two-factor authentication [59]. Also, experts have better success in managing their own passwords and they have awareness of specific threats [13].

Table 2.1: A summary of the effect of education on password behaviour.

- Experts have more unique passwords and reuse less passwords than non-experts.
- Experts use password managers more than non-experts.
- Experts write less passwords down than non-experts.
- Non-experts are not aware of prominent password managers, but they save passwords in browsers.
- Non-experts have lack of understanding of the security benefits of password managers.
- IT professionals reuse less passwords than general group and students.
- IT professionals use stronger passwords than general group and students.
- IT professionals use secure behaviours and have confidence in computer security knowledge.
- Educating users is a major initiative to enhance credentials security.

2.4 Proposed Solutions for Password Management

As mentioned previously, passwords are still preferred because it is easy to use, however, people do not handle passwords safely. People create their own passwords that easy to guess, they include personal information, create short passwords, and reuse passwords in multiple accounts. So because of these problems with password management, some solutions were designed and implemented in order to help people create strong passwords as well as tackle password reuse and short passwords. This section investigates the benefits of password policies, password strength meters and single sign-on (SSO).

2.4.1 Password Policies

Password policy is a set of requirements that was designed to encourage users to employ strong passwords, for example, at least 8 characters, the use of upper-case and special characters. In a study about password policies that examined people's behaviour, it was found that the majority of participants cope with changing passwords by modifying their current passwords, which means that the expiration policy does not influence people to create strong passwords, therefore it will not add protection against an automated guessing attack. The researchers found that 67% of participants created new passwords by only altering previous passwords, for example by capitalizing a letter in a new password [12].

Inglesant and Sasse stated that password policies frustrate users when they cannot comply with it, so users use coping strategies [60]. Also, users were annoyed by new policies and struggle to comply with it even though they believe policies provide security [49]. According to Stobert and Biddle, 41% of participants include at least one piece of personal information in their passwords, and almost half of participants stated that they look for a particular digit or capitalize a letter to comply with password policy [13].

Furthermore, Seitz *et al.* explore the top 100 websites in Germany to find out if diversity in password policies prevent password reuse [61], they found most websites require

length of 6 to 8 characters, while all tested websites allowed lowercase and uppercase letters and digits. However, they claim that password policies were never designed with the intention to prevent password reuse, therefore it fails to prevent it [61]. In an empirical study of 50 password policies (20 policies mainly from USA and 30 from mainland China), researchers found that the password policies used in the websites are vulnerable to targeted online guessing attacks [62]. They added that 60% of websites impose a minimum length to be no shorter than 6 characters, while 30% of the websites require passwords that are not shorter than 8 characters in length. They also found that English websites use stringent password policies compared to Chinese websites [62].

Moreover, Das *et al.* examined leaked passwords to measure the reuse of password, the results show that different websites apply different policies which result in mitigating the exact reuse of passwords; yet, users use tricks to work around password policies in different websites [63]. Yıldırım and Mackie conducted a study with the aim to find out whether users can create a strong and memorable password if they are not enforced to comply with password policy. They found that users who received password guidelines and sample password methods created stronger and memorable passwords than users who received password guidelines that have strict policy rules [64].

Lastly, researchers stated that increasing the number of rules and obliging users to comply with these rules caused frustration even though the restriction increases the security of password [65]. Thus, although password policies were designed to help create strong passwords, the policy for some websites is vulnerable. Also, users only modify their current passwords to cope with the policy and it causes frustration as well.

2.4.2 Password Strength Meters (PSM)

A password strength meter is an indicator that shows the strength of a password when a user enters it in a form, the strength could be in colour or text only. A finding from a laboratory experiment shows that the presence of password meters lead users to produce

strong passwords when they are forced to change their passwords for important accounts [50]. In a recent study for password creation using whitebox-based visualisations [66], researchers stated that radar chart affected the password strength in the short term and encouraged users to create passwords with digits. Also, they highlighted that password meter can affect password strength positively in the short term [66]. Ur *et al.* developed a data-driven password meter which uses neural networks and heuristics to generate data-driven text feedback, they found that this approach leads users to create more secure password than a password meter bar as well as the password is no less memorable [67].

The presence of password meters changes users' behaviour because stringent meters lead users to make password longer and add additional characters [68]. However, the scoring systems of meters that observed in the wild, e.g., Yahoo were most similar to the non-stringent meters, which suggests that the current password meters in popular websites are not aggressive enough to motivate users to create strong passwords [68]. Similarly, the password strength meters used are highly inconsistent which fail to provide solid feedback and sometimes provide misleading password strength, for example, a password labelled as weak could be strong in another website [69]. Golla and Dürmuth speculated many reasons that websites are not applying better password meters, for example, the lack of awareness and guidance on the meter's quality [11].

Therefore, we can see that password strength meters can guide users to create a strong password, but the strength meters are not good enough because they are different from one website to another (not consistent) and they could mislead users.

2.4.3 Single Sign-On (SSO)

Single sign-on is a free authentication method that allows users to access several applications with only one login (authentication), thus, there is no complexity when a user wants to access different websites with the same credential. Users are familiar with big technology companies such as Google and Twitter which offer SSO services to save users' effort

from having more accounts and remembering passwords [70]. However, researchers identified factors that hinder participants to use single sign-on (SSO), for example, participants have trust concerns and express concerns about phishing attack [71]. Also, SSO OpenID is not resilient to phishing attacks and internal observation [72]. The other problem is that it is only offered by specific services such as Gmail and Twitter, so not every website accepts SSO for authentication although SSO reduces the number of passwords needed.

2.4.4 Two-Factor Authentication (2FA)

To increase the security of online accounts and prevent any access to the online account by an unauthorized person, two-factor authentication (2FA) method was introduced. Two factor authentication method is used by companies such as Microsoft and Google and password managers as well, the method can be something you have, e.g., phone or hardware token, or something you are, e.g., Biometric [73]. It was stated that the use of hardware token (RSA SecureID) and mobile phone (Phoolproof) are resilient to many attacks such as guessing, internal observation and phishing attacks [72]. However, the schemes cannot be recovered if lost, and they are not scalable nor memory efficient [72]. Each user might need a separate token for each account and need to generate a PIN code every time they want to access the website. More importantly, using two-factor authentication does not eliminate passwords at all because passwords are still required to register and login to online accounts.

2.5 Password Managers (PM)

We can see that many solutions have been proposed to help people manage their own passwords, but these solutions have limitations that make it harder for people to handle their own passwords. People need a solution that stores their own passwords, generates a strong random password, and recalls them when needed, all of which come in the form

of a password manager. Password manager is a tool that was developed to help people manage their own passwords, generate a unique password and prevent password reuse. Password managers store online passwords; thus users do not need to memorize them nor write them down. Also, some password managers offer other features such as storing bank details and driving licence. There are different types of password managers; browser-based password manager, e.g., Chrome [74], cloud-based password manager, e.g., LastPass [75] and open-source password manager, e.g., KeePass [76].

2.5.1 Benefits of Password Managers

Writing passwords down in a secure place or using password managers can be a promising solution to password reuse problem [55]. Password manager improves usability by auto-filling the login form and stored passwords are synchronized over user's devices based on cloud [77]. Pearman *et al.* conducted an interview study and found that users of separate password managers seem to be driven by its security, while users of built-in password managers might be driven by its convenience [78].

A password manager generates, stores, and fill in the user's passwords while the user has one master password [79]. Users create stronger passwords when they use memory aids which could encourage them to use password managers [80]. Besides, password managers offer the benefits of having strong passwords and uniqueness, while users of password generator mostly have stronger password and reuse less passwords [81]. Password managers become popular to generate strong passwords for many accounts and prevent password reuse [82].

2.5.2 Problems with Password Managers

However, there are some problems in password managers. Previous work [46] stated that third-party password managers do not reduce password reuse, while another study

[47] found that neither password managers nor autofill functionality significantly affected password reuse or password strength. Also, researchers found that the autofill functionality of the Chrome browser exacerbated the passwords reuse problem, while 53% of entered passwords with LastPass password manager were not reused [81]. The result of study [81] confirms the result of [46], [47] that found password reuse is rampant.

In a study about adopting and rejecting smartphone password managers, the results show a number of rejecting factors such as usability, no awareness, privacy issues, security concerns, device memory and battery, and control [83]. Similarly, the lack of immediacy and lack of time are the most common reasons for not downloading and using password management applications [84]. Some participants do not use password managers as they have a lack of trust (44%) and no need for it (36%) [13]. In a further study about passwords, participants expressed few concerns about using password managers such as the risk of the database getting hacked, failure of the software or accidental password loss [40]. Also, it was found that trust is only partially significant in password managers [85].

Fagan *et al.* investigated the difference between users and non-users of password managers, they found that users of password managers have more accounts and unique passwords, they have higher computer proficiency and better experience in computer security than non-users [86]. In contrast, non-users have security concerns with password managers, a lack of need and a lack of understanding of the benefit of the tool [86]. Fagan and Khan conducted a study [87] using the security advice from study [55], and concluded that a large number of non-users view it as a security risk, but users of a password manager use it because of its convenience, e.g., autofill and others said it added security [87].

In addition, Stobert and Biddle said that a password manager is a single point of failure because all stored accounts will be compromised if a master password is lost [14]. Also, attackers will have control of all the users' accounts if they have access to a master password [79]. Earlier in 2019, it was reported that researchers at Independent Security Evaluators (ISE) found the Windows 10 app for five popular password managers (Dash-

lane, 1Password, LastPass, KeePass and RoboForm) have a security flaw when the apps are in locked mode, as some passwords were left exposed in the computer's memory [88]. Carr and Shahandashti analyzed five popular password managers and found that they are vulnerable to attacks, for example, Keeper, Dashlane and 1Password were vulnerable to user interface (UI) driven brute force attack, while the Android applications for 1Password and LastPass were vulnerable to a phishing attack [89].

Furthermore, password managers introduce a single point of failure even though it improves usability for not remembering and typing passwords [2]. In a study about the security of open-source password managers, it was stated that users have to trust closed source password managers to store passwords securely because they do not know how their passwords are stored and processed [9]. In a recent study, Ray *et al.* said that older adults do not trust the synchronization in separately installed password managers, and they do not trust them to store passwords in cloud as they want to have more control [90].

Gasti and Rasmussen performed a security analysis in the database of different types of password managers such as Google Chrome, Firefox, 1Password and Roboform [20], they found that the database formats of most password managers are vulnerable and broken even against weak attacks. They advised users to carefully consider storing their own passwords in an acceptable database, either store in a cloud, USB drive or a shared machine between users [20]. Also, another study found that the autofill feature in password managers can result in catastrophic consequences due to a remote network attack [22].

Zhao *et al.* performed a security analysis using a threat model to evaluate LastPass and RoboForm [19], they found that the master password is optional in RoboForm, while LastPass remember and save the master password in the local device. Users should be instructed to use a strong master password, while remembering and saving the master password of LastPass in the local device can lead to a security problem [19]. Additionally, Li *et al.* conducted a security analysis of web password managers and found key security concerns; they found vulnerabilities in features such as bookmarklet, share passwords as well as the attacker can steal users' credentials [17].

Table 2.2: A summary of factors that affect password behaviour.

- Third-party password managers do not reduce password reuse significantly.
- The use of autofill functions or password managers do not have discernible effects on password strength or password reuse.
- The autofill functionality of Chrome exacerbated the passwords reuse problem.

Table 2.3: A summary of factors that affect the adoption of password managers.

- Lack of awareness as people do not know about password managers.
- Lack of understanding of the benefit of password managers and lack of need.
- Security concerns towards password managers, such as hacking the database and security flaws in the apps.
- A single point of failure because all stored passwords will be compromised if the master password is discovered.
- Privacy concerns towards the developers and the software.

2.5.3 Solutions for Password Managers

As stated in the previous section, password managers have usability and security problems, as a result, researchers proposed different solutions to solve these problems, such as the problems with master password. McCarney *et al.* proposed Tapas password manager which encrypts and stores passwords on a smartphone, while decryption keys are stored on a user's paired computer. The purpose of using a computer and a smartphone is to be a theft-resistant system without the use of a master password [15]. Similarly, BluePass password manager stores user's passwords on a mobile device, while decryption keys are stored on BluePass own server and a trusted computer, and the user uses a master password to retrieve the keys from BluePass server. So, compromising the master password is meaningless because passwords are stored separately on a mobile device. Also, BluePass uses Bluetooth to communicate between a smartphone and a computer [16].

Moreover, Fukumitsu *et al.* proposed a framework for password manager that used secret sharing and a personal server. The idea is that the login information will be stored

as shares in a computer (PC), a smartphone and a server. So, the user can recover the login information if they have two devices, meanwhile it is theft resistant because an attacker needs to compromise two devices to have the login information [91]. Furthermore, SplitPass password manager splits a password into two halves (parts), a half is stored on a device, while the other half is stored on a cloud assistant. The device will not get access to the other half that is stored on the cloud assistant and vice versa but the process is still transparent to the server [18].

Amnesia password manager generates a password on demand using a master password and the information on a user's smartphone. So, it is not vulnerable to a database leak because the attacker has to compromise the master password and the user's smartphone, or Amnesia server and the user's smartphone [92]. In a recent study by Stobert *et al.*, they designed ByPass which provides a secure and direct communication between the website and the manager. ByPass improves usability and minimizes users' interaction to complete tasks as it supports functionality such as an automated password change and minimizes errors [93].

Also, UniPass password manager was designed for visually impaired users (participants who are blind and those with low vision). The idea of UniPass is to authenticate a user to a smart device, where their credentials to be used on another device such as a computer. The researchers found that the majority of impaired participants preferred UniPass over LastPass and StrongPass password managers [94]. Another password manager was proposed, which addresses the issue with password managers that do not hide the master password or passwords from itself. HIPPO password manager does not know or store the master password or web passwords because it computes a unique password for each service by receiving the key from a server and the master password from the user [95].

Yang *et al.* proposed a cloud password manager scheme using two factors which are biometrics and a master key. This scheme is efficient and secure for password manager service that are hosted by untrusted cloud service providers because it relies on a cloud service to synchronize all clients of a password manager in an encrypted form [21].

Table 2.4: A summary of the proposed password managers by researchers (section 2.5.3).

Password Managers	Summary
Tapas [15]	It does not use master password. It stores passwords on a smart-phone and stores decryption keys on a paired computer. It is a theft-resistant system that does not require a master password.
BluePass [16]	Master password is used to authenticate a user to BluePass server and to retrieve decryption keys. It stores passwords on a smart-phone and stores decryption keys on own server, but for a long term on a trusted computer. It uses Bluetooth for communication.
SplitPass [18]	It splits a password into two halves, a half is stored on a device and the second half is stored on cloud assistant. The process is transparent to the server. The device will not have access to the second half that is stored on the cloud assistant and vice versa.
Fukumitsu <i>et al.</i> [91]	It uses secret sharing scheme. Login information are stored as shares in a computer, a smartphone and a personal server. The user can recover login information if they have two devices out of three. The attacker needs to compromise two devices to have the login information, so the framework is theft-resistant.
UniPass [94]	It is designed for visually impaired users. It authenticates a user to a smart device and their credentials to be used on another device such as a computer.
Amnesia [92]	It generates website passwords on demand using master password and the information on a user's smartphone. It is not vulnerable to a database leak as an attacker has to compromise both the master password and the user's smartphone, or both Amnesia server and user's smartphone.
HIPPO [95]	It addresses the problem with password managers that do not hide the master password or passwords from itself. HIPPO does not know or store the master passwords and web passwords. It computes a secure password for a website by receiving the master password from the user and a key from the server.
ByPass [93]	It provides a secure and direct communication between the website and the manager. It improves usability and minimizes users' interaction to complete tasks because it supports functionality.
Yang <i>et al.</i> [21]	It uses biometrics and a master key, and relies on a cloud service to synchronize all clients of a password manager in an encrypted form. This scheme is efficient and secure for password manager services that are hosted by untrusted cloud service providers.

Also, a recommender application was designed to encourage the adoption of password managers in which the researchers found that offering choices to support autonomy and using non-controlling language encouraged more users to use password managers. However, 70% of participants did not install password managers because of trust issues and it

takes time to set up [96].

Additionally, it was suggested that password manager would be open-source so those who use it will know how their privacy is protected, while the master password must be strong and should be complex that meets the 2017 NIST standards [9]. Researchers [46], [47] suggested that the current forms of password managers might not be complete solution, while it was suggested that integrating password managers into browsers and operating systems to help with trust and visibility [13]. Usability improvement are suggested in password managers before recommending them to users, as usability drawbacks in password managers are harder to deal with for non-experts [55].

Oesch and Ruoti recommended that password managers adopt strict requirements for master passwords as well as require user interaction before autofilling their passwords [97]. In a recent study, it was found that mistrust is a strong reason for rejecting smart-phone password managers and they are barely acceptable, so there should be improvement to security, user guidance and interaction [98].

2.5.4 Technology Adoption Life Cycle

As stated earlier, technology has become important in people's life and more devices and applications have been developed in the last decades which make it more flexible for people to do many things online. The technology development increases the number of online accounts which means more passwords to create and memorize. Passwords are very important and sensitive as they are protecting online data, but because of insecure practices that have been used by people, different solutions have been proposed to solve password management problems, and one of these solutions is a password manager. In order to try and adopt a password manager as a new technology, people will go through different stages at different rates to accept, adopt and use the new technology or reject it.

In 1956, Beal and Bohlen [99] stated that people accept new ideas after a series of complex mental processes which consists of 5 stages (awareness, interest, evaluation,

trial and adoption). Also, the researchers said that people adopt new ideas at different time, while other people never adopt them [99]. Other researchers focused on smartphone application adoption life cycle for password managers [83]. They stated that the life cycle has influencing factors which are search, decide, trial and finally adopt the application or reject it during these phases. The phases in study [83] are quite similar to the 5 stages that suggested by [99], therefore, I will focus on the adoption life cycle by [99] because [83] only focuses on smartphone.

Also, Davis [100] developed a model regarding accepting and using new technology which is “Technology Acceptance Model”. This model is about the usefulness of the technology that enhances job performance of an individual, as well as the ease of use of the system in which using it is free of effort. This model covers the aspects of usefulness and ease of use which can be relevant to users of password managers in terms of ease of use of the programs. So, these models [99], [100] of adopting and accepting a new technology can be applicable to password managers, because they are covering the aspects of awareness, evaluating, adopting and using a new technology.

Previous studies found factors that lead to the rejection of password managers, such as lack of awareness [83], lack of awareness and knowledge [78], and insufficient awareness of how to install and use the technology and how it works [84]. Other factors that affect the adoption of password managers are lack of trust [13], [90] and security concerns [40], [86]. However, researchers [55] found that experts use password managers more than non-experts. Moreover, the usability of password managers can be a problem that makes people refrain from using them.

Based on the adoption life cycle [99], lack of awareness and knowledge can be in the awareness stage because people do not know what a password manager is. People who do not know how to install a password manager and how it works can be in the interest stage because they are looking for more information about the program and the idea. Regarding those who have lack of trust and security concerns about password managers, they can be in the evaluation and trial stages because they are in the stage of making a mental trial

of a password manager and how it can help them store and manage passwords. For users of password managers, the adoption stage [99], as well as the ease of use of the program [100] apply to them because they are using password managers.

Furthermore, part of this research concentrates on the educational background of users and non-users of password managers (chapter 5), and whether having educational background in computer science or information security will play a significant role in the adoption rate of password managers, using password managers or not adopting the programs at all. In the discussion chapter (section 8.2), we discuss which stage of the adoption life cycle that our participants have reached.

2.5.5 Call for Further Investigation

Researchers stated that many password managers and browsers do not prevent passwords reuse, thus it should be investigated further while preserving a positive user's experience [101]. The results of previous studies indicated that password managers have no effect on password reuse [46], [81] and do not have effect on password strength and reuse [47]. Also, researchers called for more focus on non-expert users, better design for password managers and explore how education and advertising can target people with less experience in technology and those who do not use password tools [78].

Lyastani *et al.* suggested further investigation to understand and tackle the issues why users abstain from using password managers [81]. It was suggested that users might be reluctant to use password managers because of an ingrained mental model, e.g., should not store password [55]. Chaudhary *et al.*, stated that some studies are inconsistent, thus the research results contradict each other in many cases which might confuse someone who wants to design a password manager. The reason is that an issue that was identified as a problem in one article is not considered as a problem in another articles [5]. Lastly, the role of trust in password managers can be investigated further in future research [85].

2.6 Conclusion

To conclude, people are still relying on passwords and using them widely to authenticate themselves to online accounts which implies that passwords will dominate for many years to come. Unfortunately, people use insecure practices to handle their own passwords, they create guessable passwords, reuse them in multiple accounts as well as they cannot remember their passwords. To mitigate these problems, a password manager was designed which can be a promising and suitable solution. However, previous studies have predominately focused on passwords or on the technical and security side of password managers such as [7], [10], [13]–[22] or on smartphone password managers [83], [98], but rarely on the human perspective and usability of password managers.

Consequently, it is unclear why non-users do not use password managers even though they are widely available, is the low adoption related to usability problems, trust issues or security concerns? Previous studies have rarely focused on users of password managers in which I believe that users might have similar issues as non-users in terms of usability, trust, security, and transparency. Also, to the best of my knowledge, there is no study that has evaluated the user interfaces and usability of cloud-based password managers which can be a possible reason that discourages people, particularly non-users, from using them due to their design and the use of specific functions.

Therefore, I look at the human perspective in the use and non-use of password managers in terms of four key aspects (usability, trust, transparency and security) which in chapters 4 and 5, while I investigate about the user interface and usability of cloud-based password managers using Nielsen's 10 principles in the next chapter.

Chapter 3

Evaluation of Password Managers

Using Nielsen's 10 Principles

3.1 Introduction

Jimenez *et al.* [102] stated that there are several methods to assess the usability of interactive software systems, and heuristic evaluation is one of the most accepted methods. Research has shown that detecting problems early in the development of a software product can help to ensure the quality, reduce service costs of post-release and save money [102]. So, to investigate the user interface and usability of cloud-based password managers (LastPass, Dashlane and Keeper), I used Nielsen's principles (heuristics). Nielsen's 10 principles are useful and helpful to evaluate the design of programs, identify issues in user interfaces and usability problems that impact the overall user experience, also, to identify the positive aspects of the programs.

In the 1990s, Nielsen's 10 principles were developed as user interface design guidelines, which have been reflected in the design of products by companies such as Google and Apple [103]. 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" [104]. Nielsen's 10 heuristics have been the most accepted and applied, while new specific usability heuristics have been developed to improve the outcome of usability evaluation [102].

Nielsen's heuristics are made of 10 usability principles that shed more light on the usability and user interface of systems which are helpful to inspect current cloud password managers. In fact, there are other heuristics available such as Schneiderman's 8 golden rules of dialog design and ISO's 7 dialogue principles. Nielsen's principles offer more insight into "aesthetic and minimalist design" and "help and documentation" which do not exist in Schneiderman's rules. Also, ISO does not have an important principle which is "help users recognize, diagnose and recover from errors" along with the other two principles that Schneiderman does not have.

Therefore, Nielsen's 10 usability principles are the suitable heuristics to follow in this study, because Nielsen's principles cover extra aspects and these extra aspects matter for password managers. For example, "help and documentation" shows the users how to install the program and store passwords, while "aesthetic and minimalist design" is for the layout of programs. The principle "help users recognize, diagnose and recover from errors" is important as it shows error messages (warning) about problems that are related to passwords and other areas in the programs.

The results of this study show that the user interface design of these password managers are visible, consistent and aligned. Regarding usability, these password managers give users control as well as they are flexible and efficient to use to some extent. LastPass, Dashlane and Keeper offer many features such as storing many passwords and personal information. They provide concrete icons, speak the user's language and they fill in credentials automatically which saves time. On the other hand, the three password managers have some problems, for example, there is no undo function when a user saves new changes. These managers do not prevent a user from inserting incorrect data, while they use computer jargon. Also, it is difficult to recover the account in LastPass and Dashlane, while the master password requirements are not strong enough.

3.2 Methodology

The evaluation of password managers will help to gain an insight into a program and its user interface and suggest solutions to improve it. The evaluation is divided into two parts, a positive part which explains the good points about the program, and a negative part where problems are identified and explained, along with recommendations to solve these problems. The evaluation goes through four different stages: a training and briefing session about which tasks the evaluators will focus on, evaluating the user interface and usability of the program and applying heuristics, record problems and explain them along with the severity ratings, and finally, a debriefing session to suggest solutions for these problems (brainstorming). An evaluator who should be an expert (not any user) inspects the user interface and the usability of the program, compares it to the heuristics so that they can list usability problems and then explains each problem and suggests solutions [103], [105], [106].

In this section, I conduct an evaluation of three cloud password managers (LastPass, Dashlane and Keeper) by myself using Nielsen's 10 principles. More precisely, I evaluate the user interfaces of three password managers and their main functions and features, such as storing passwords, creating master passwords and recovering password manager accounts. To the best of my knowledge, this study is the first evaluation of the user interfaces and usability of cloud password managers using Nielsen's principles. The use of Nielsen's principles will answer the first question of this research: "Do the usability and user interface design of current cloud password managers satisfy Nielsen's 10 principles?"

The definition of the principles are taken from two sources because they complete each other and are easier to access [28], [29], while all checklists can be found here [29]. I evaluate cloud password managers because they have many features and functions; LastPass is one of the most popular cloud password managers and it has many free features, while Dashlane and Keeper are also popular password managers with many features. I selected three password managers to evaluate because they were mentioned within the best

password managers [107]–[114]. The evaluation was conducted in the middle of 2019.

Table 3.1: Nielsen’s 10 principles and definition [28], [29]

	Principles	Definition
1	Visibility of System Status	The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
2	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.
3	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.
4	Consistency and Standards	Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.
5	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.
6	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.
7	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.
8	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.
9	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.
10	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 limitation in this study is that Nielsen recommended to have between three to five evaluators, while I evaluated the three cloud password managers by myself. The reason I evaluated these password managers by myself is that training people from the university or hiring external evaluators to conduct the evaluation will be time and money consuming. However, Wong [103] stated that in the early stages of development, it is often sufficient to have one or two evaluators to identify the majority of usability problems.

3.3 Result

In this study, I evaluated popular password managers (LastPass, Dashlane and Keeper) using Nielsen's principles. Table 3.2 shows a summary of the features of the free windows versions of these password managers in 2019. Also, table 3.3 shows a summary of the features of other popular password managers in 2022 such as 1Password and Zoho [115].

- **LastPass password manager:** The most popular cloud-based password manager that has its own browser extension and webpage. The evaluation of LastPass was conducted using free Windows versions (starting from version v4.30, and the findings are confirmed between versions v4.31 to v4.33.5).
- **Dashlane password manager:** This is a cloud-based password manager that has its own desktop application, browser extension and webpage. Dashlane has limited free features compared to LastPass. The evaluation of Dashlane was conducted using free Windows versions (starting from version 6.1926.1, and the findings are confirmed between versions 6.1929.1 to 6.1935.0).
- **Keeper password manager:** This is another cloud password manager which has its own desktop application, browser extension and webpage. Keeper has fewer features than Dashlane and LastPass. The evaluation was conducted using free Windows vault versions (starting from version 14.5.1, and the findings are confirmed by version 14.9.2). The extension versions (from 12.3.7, 12.4.1 to 12.5.2).

Table 3.2: A summary of popular password managers in 2019.

Password Managers	Summary
LastPass	<ul style="list-style-type: none"> • It stores an unlimited number of passwords, offers two-factor authentication and auto-fill feature. • It stores personal information and supports passwords synchronization between devices. • It offers a password generator, free to use browser extension and users can access passwords from the webpage. • LastPass offers other features such as revert master password and multifactor choices.
Dashlane	<ul style="list-style-type: none"> • It stores up to 50 passwords, offers two-factor authentication and auto-fill feature. • It stores personal information, and it synchronizes passwords across user's devices (sync not free). • It offers a password generator, free to use browser extension and users can access passwords from the webpage, but users have to install the desktop app to use the features. • It offers a password changer that changes passwords automatically with one-click.
Keeper	<ul style="list-style-type: none"> • It stores many passwords, offers two-factor authentication, and it stores personal information. • It allows users to access their own passwords from the desktop application. • It offers a password generator within the program, but not as a separate tool such as in LastPass and Dashlane. • In the free version, users cannot use browser extension or auto-fill feature and users cannot access passwords from the webpage.

Table 3.3: A summary of other popular password managers in 2022 [115].

Password Managers	Summary
1Password [116]	<ul style="list-style-type: none"> • It does not have a free version, but only offers a 14-day trial. • It allows users to store an unlimited number of passwords, offers two-factor authentication and auto-fill feature. • It allows users to synchronize passwords across an unlimited number of devices, and it stores personal information. • It offers a password generator and browser extension. • 1Password provides users with a secret key. The users need the secret key each time they add a new device or browser extension.
Bitwarden [117]	<ul style="list-style-type: none"> • The free plan of Bitwarden allows users to store an unlimited number of passwords, offers two-factor authentication and auto-fill feature. • It also allows users to synchronize an unlimited number of items between their own devices, and stores personal information. • It offers a password generator and browser extension. • It offers credential sharing feature.
Zoho [118]	<ul style="list-style-type: none"> • It has a free plan which offers unlimited password storage and allows passwords synchronization across devices. • It offers auto-fill feature and two-factor authentication. • It stores personal information, offers a password generator and browser extension.
RoboForm [119]	<ul style="list-style-type: none"> • The free tier offers unlimited password storage, multi-platform support and login sharing. • It stores personal information, offers a password generator and it allows users to fill in data. • RoboForm Everywhere, which is not free, offers two-factor authentication and allows data synchronization across devices.

In the next sections, the positive aspects (section 3.3.1) and the negative aspects (section 3.3.2) of the three password managers (LastPass, Dashlane and Keeper) are presented and explained using Nielsen's 10 principles. In table 3.4, the positive aspects of the three password managers are shown along with the applied principles, while table 3.5 shows the negative aspects (problems) of the three password managers along with the violated principles and severity rating.

3.3.1 Positive Aspects of the Three Cloud Password Managers

Table 3.4: Positive aspects and Nielsen's principles applied to three 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)	Visibility of system status. Aesthetic and minimalist design.
All 3	Copy and modify data	User control and freedom. Flexibility and efficiency of use.
All 3	Autofill credentials to log in	Recognition rather than recall. Flexibility and efficiency of use.
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 (warning)	Help users recognize, diagnose and re- cover 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	Account settings	Visibility of system status. Consistency and standards.
LastPass	Different paths to find functions	Flexibility and efficiency of use. User control and freedom.
Dashlane	Password changer	Flexibility and efficiency of use.

Dashlane	Tools	Visibility of system status. Aesthetic and minimalist design. Consistency and standards.
Dashlane	Different paths to find functions	Flexibility and efficiency of use. User control and freedom.
Keeper	Recover account	Flexibility and efficiency of use. Help users recognize, diagnose and recover from errors.
Keeper	Settings	Visibility of system status. Aesthetic and minimalist design. Consistency and standards.

Explanation of the 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, which is on the left side, 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 dialog boxes which have an entry data field in the system. Each dialog 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 in LastPass, while personal information field is different to payments in Dashlane.

Storing online passwords: There is a specific dialog box for each account/password, the user can fill in accounts and passwords, categorise them into groups such as social media 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 which is clear, brief and aligned, which shows what users need to see (visual icons with titles), this is where a user can categorise stored data and use a grid view or list/large view to organize them. When the user adds new information or changes it, the system will show a notification (especially LastPass and Keeper). Please note that Dashlane and Keeper have a webpage and desktop app which have the same design.

Copy and modify data: The three password managers allow the user to copy password and paste it on the login form and in a dialog 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 login form, so the user does not need to type these, which saves time. If the user has multiple accounts on the same website (e.g., Twitter), then these password managers will show a drop-down list of Twitter accounts in login form so the user can choose an account from the list. Please note that the extension has to be installed and enabled to use this feature.

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, such as changing a phone number, resetting a master password

or changing the security question in Keeper.

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 (browser extension needs to be enabled). Dashlane shows the strength of a password generated in words and colours (unlike LastPass). However, Keeper only has a random password generator embedded in the password section, so it is not a separate tool as in LastPass and Dashlane.

Error messages (warnings): The three password managers use very clear text to inform users about errors and indicate what need to be done. The error message is shown briefly and unambiguously and does not criticize the user for anything. For example, LastPass alerts users if a password is reused on another website and suggests a solution. Also, the systems warn the users if they are about to make a potential destructive actions, for instance, Keeper asks users for confirmation before deleting a record from the vault.

Log in to main page (vault): The three password managers open the main page (vault) to the user once the correct email and master password are submitted on the login form (the webpage/app). 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 on how to use the system. Instructions are divided into different sections such as installation for Dashlane, explore features for LastPass and user guides for Keeper password manager.

Different paths to find functions (LastPass/Dashlane): The random password generator can be found in different places which is in browser extension, webpage (LastPass) and in the desktop app (Dashlane). This makes it flexible to open it more quickly. Also, users of LastPass can find account settings in the main menu and in the drop-down menu.

Account settings (LastPass): The majority of settings and features are presented in

one place. The user can navigate to 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 to the settings and choose a function or feature. Each feature/function will be active when the user clicks on it.

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 address and then ask the user to answer a security question. Finally, the user will reset the master password and access the account without losing any passwords.

3.3.2 Negative Aspects of the Three Cloud Password Managers

There are a few problems in LastPass, Dashlane and Keeper that might affect their adoption by people, particularly novice users and those without computer science background.

The severity ratings for usability problems are as follows [106]:

- **No problem:** I do not agree that this is a usability problem at all.
- **Cosmetic problem:** Need not be fixed unless extra time is available on the project.
- **Minor problem:** Fixing this should be given a low priority.
- **Major problem:** Important to fix, so should be given a high priority.
- **Catastrophic:** Imperative to fix this before product can be released.

Table 3.5: Problems, violations of Nielsen's principles and severity ratings for LastPass, Dashlane and Keeper.

	Problems	Violated Principles	Severity Rating
All 3	Recovery from a serious wrong action as there is no undo function when saving new changes.	Help users recognize, diagnose and recover from errors. User control and freedom.	Major
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, diagnose and recover from errors. Flexibility and efficiency of use.	Minor
All 3	Store different passwords for the same account as there is no prevention.	Error prevention. Help users recognize, diagnose and recover from errors. Flexibility and efficiency of use.	Minor
All 3	No asterisks in data entry and dialog boxes mandatory.	Recognition rather than recall. Flexibility and efficiency of use.	Cosmetic
All 3	The use of extensive computer jargon by the system.	Match between system and the real world.	Minor
LastPass	Account settings functions are not visible nor organized.	Visibility of system status.	Cosmetic
LastPass	Users can create a master password that does not match the requirements.	Error prevention. Help users recognize, diagnose and recover from errors.	Catastrophic
LastPass	Auto-change password does not work with websites and is not visible.	Consistency and standards. Flexibility and efficiency of use.	Cosmetic
LastPass	Inconvenience when generating a new password.	Flexibility and efficiency of use. Visibility of System Status.	Cosmetic
LastPass	Recovering a LastPass account is difficult as it has to be from the same device and browser and requires authentication.	Flexibility and efficiency of use. Help users recognize and diagnose and recover from errors.	Major
Dashlane	Dark colour for main menu.	Visibility of system status.	Cosmetic
Dashlane	Users can create a master password that meets strong requirements, but only by using an email address.	Error prevention. Help users recognize, diagnose and recover from errors.	Catastrophic
Dashlane	Changing the master password while synchronization is disabled causes a loss of data stored on other devices.	Flexibility and efficiency of use.	Major

Dashlane	To recover an account, it requires contacting the business team and is “not free”.	Flexibility and efficiency of use. Help users recognize and diagnose and recover from errors.	Major
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.	Minor
Keeper	Users can create a very weak master password.	Error prevention. Help users recognize, diagnose and recover from errors.	Catastrophic
Keeper	There is no random password generator in browser extension of Keeper.	Flexibility and efficiency of use.	Minor
Keeper	For free version, users can only use the app but cannot use extension nor webpage.	Flexibility and efficiency of use.	Minor

Explanations of problems and recommendations in the three password managers:

Recovery from a serious wrong action as there is no undo function when saving new changes: In the three password managers, if a user removes a username or password and confirms the change, then there is no undo function for it, for example, removing the whole account in Dashlane and a username in LastPass. 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, phone number or an email address.

The recommendation to solve this problem, the three password managers should allow users to undo any actions within a specific time, for example, within 24 hours, so that they can rectify a mistake that might have been made (undo and recover from errors).

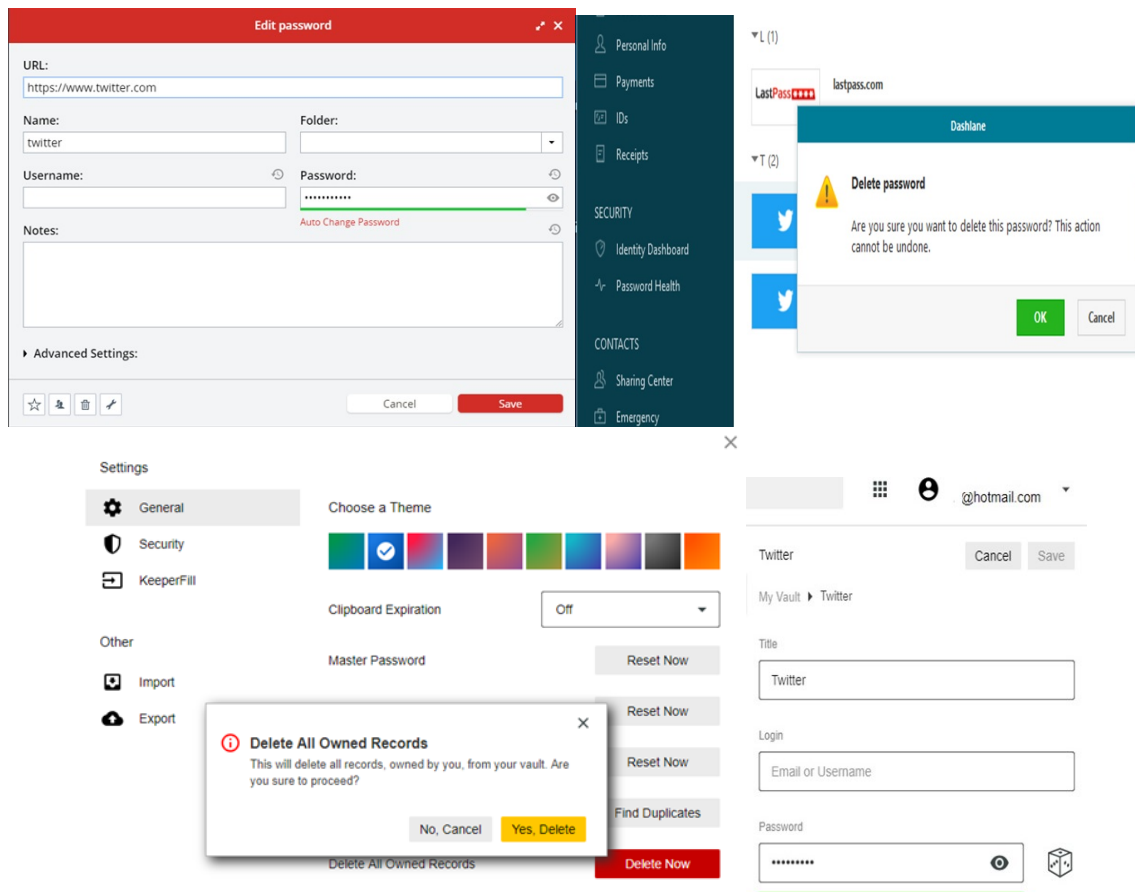


Figure 3.1: Remove username from LastPass. Remove password from Dashlane without undo function for this action. Remove username from Keeper without undo function, and no undo for deleting all records as it is a paid feature (personal email is hidden).

The system does not prevent a user from inserting incorrect data in a field or storing incomplete data: The 3 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, an incorrect long phone number and store incomplete data.

The recommendation to solve this problem is that the three password managers should prevent users from inserting incorrect URLs, long wrong phone numbers and incorrect email addresses.

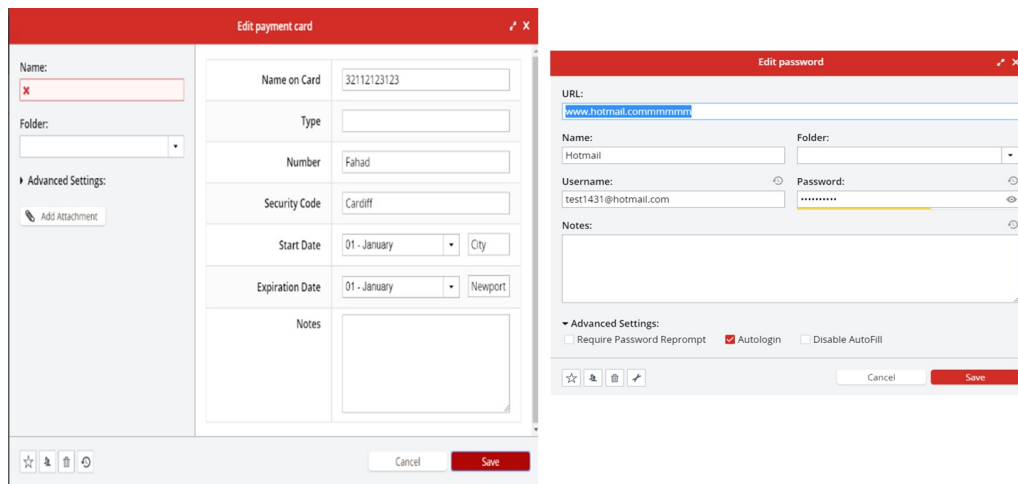


Figure 3.2: LastPass does not prevent users from storing wrong data, for example, incorrect URL, alphabetic instead of numerical characters.

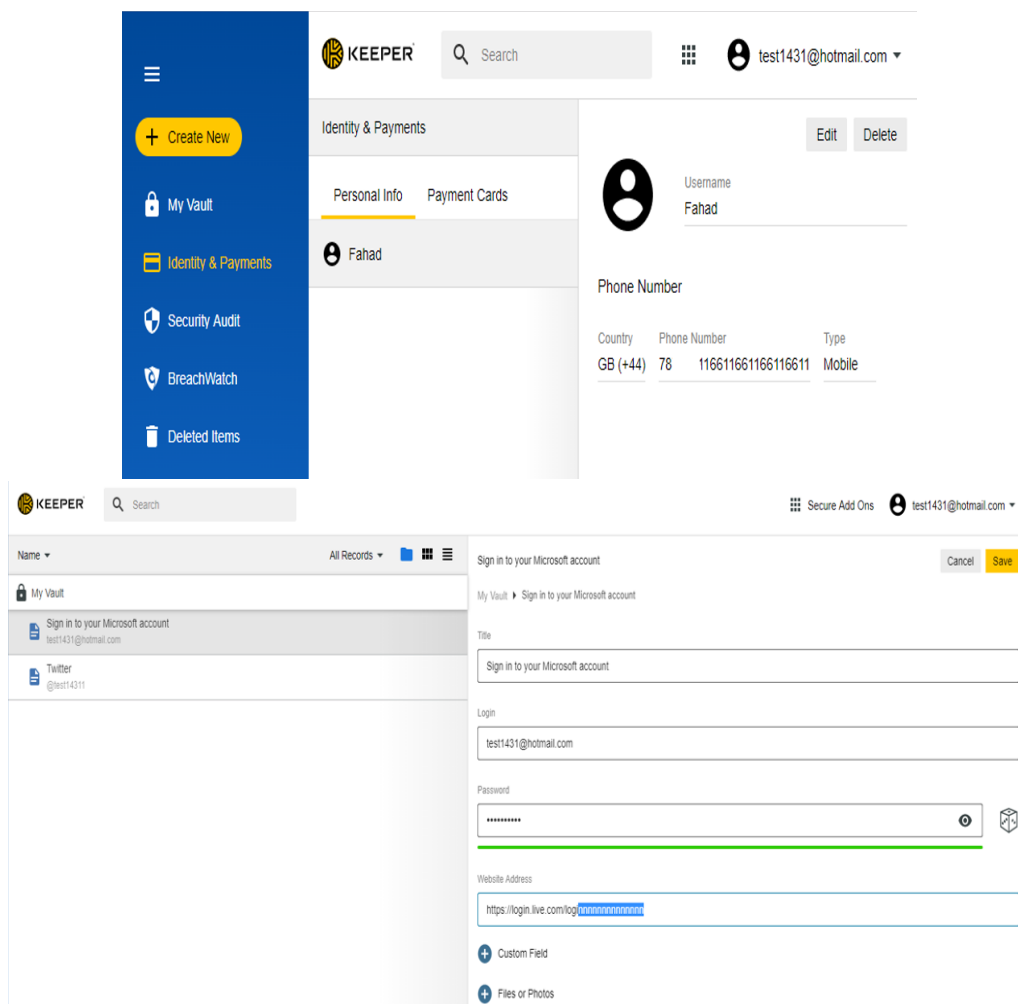


Figure 3.3: Keeper does not prevent users from storing wrong data, for example, incorrect URL and phone no (part of phone number is hidden).

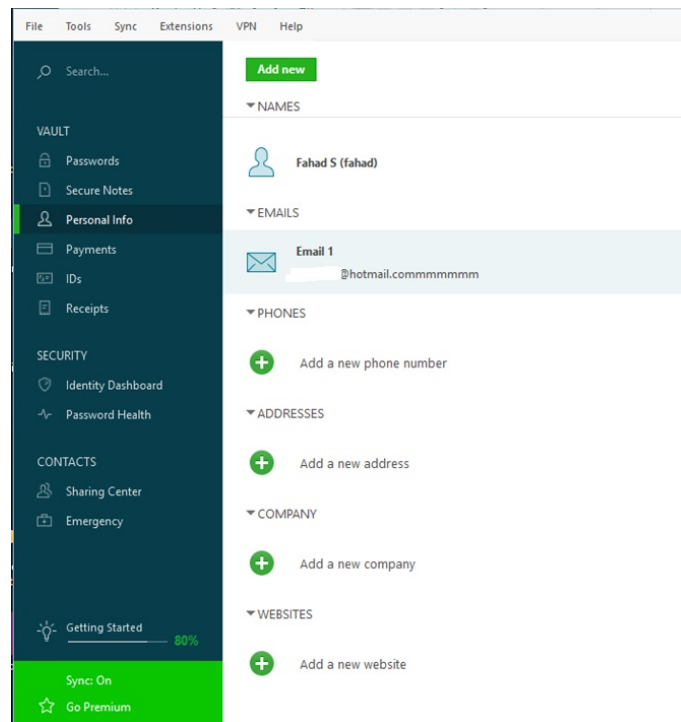


Figure 3.4: Dashlane does not prevent users from storing wrong data, for example, incorrect email address. The personal email here is hidden but you can see the wrong extension of @hotmail.commmmmmm.

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 or duplicate the 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 the correct account to use.

The recommendation to solve this problem is that 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.

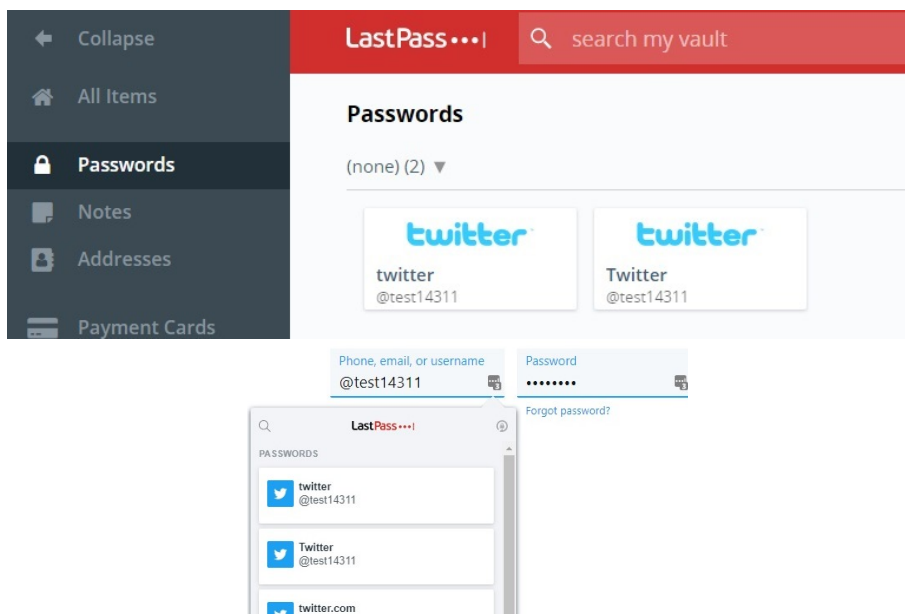


Figure 3.5: LastPass does not prevent users from storing the same account twice (with different passwords). The same Twitter account can appear twice on LastPass vault. Also, in Twitter, the autofill login form shows the account twice (from 2020).

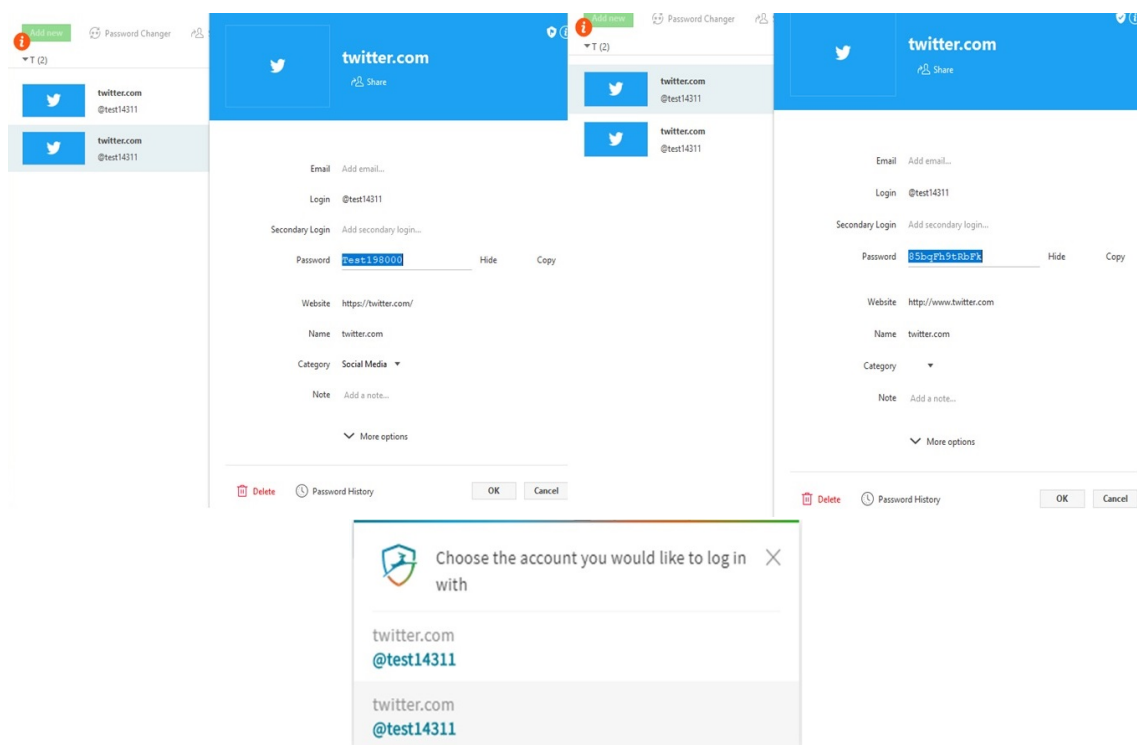


Figure 3.6: Dashlane does not prevent users from storing different passwords for the same account.

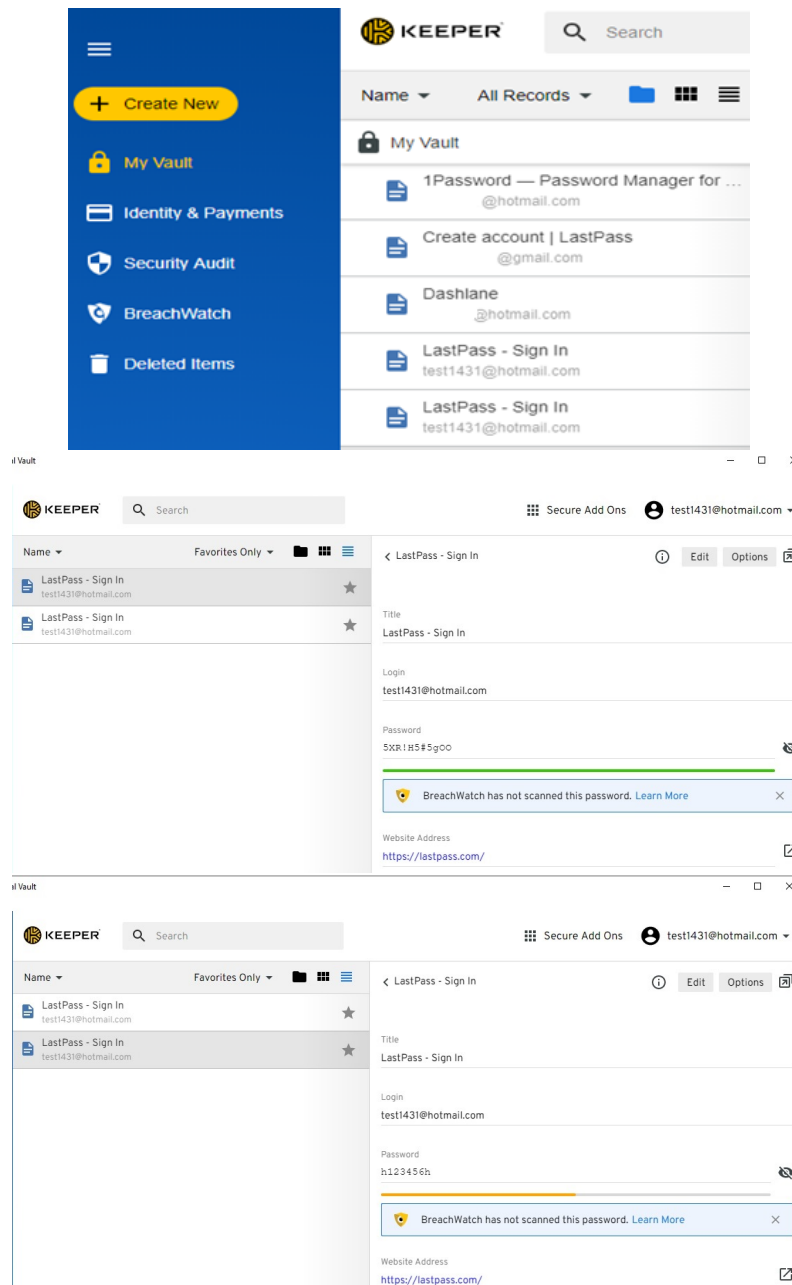


Figure 3.7: Keeper does not prevent users from storing different passwords for the same LastPass account (personal emails are hidden for other accounts). A screenshot from 2020 with a better quality.

No asterisks in data entry fields and dialog boxes mandatory: The systems do not show which data is mandatory to fill in, so users will be confused about which data they need to fill in.

To solve the problem, the 3 password managers should use asterisks for mandatory fields that need to be filled in, such as names, email and so forth, so it is clear to all users.

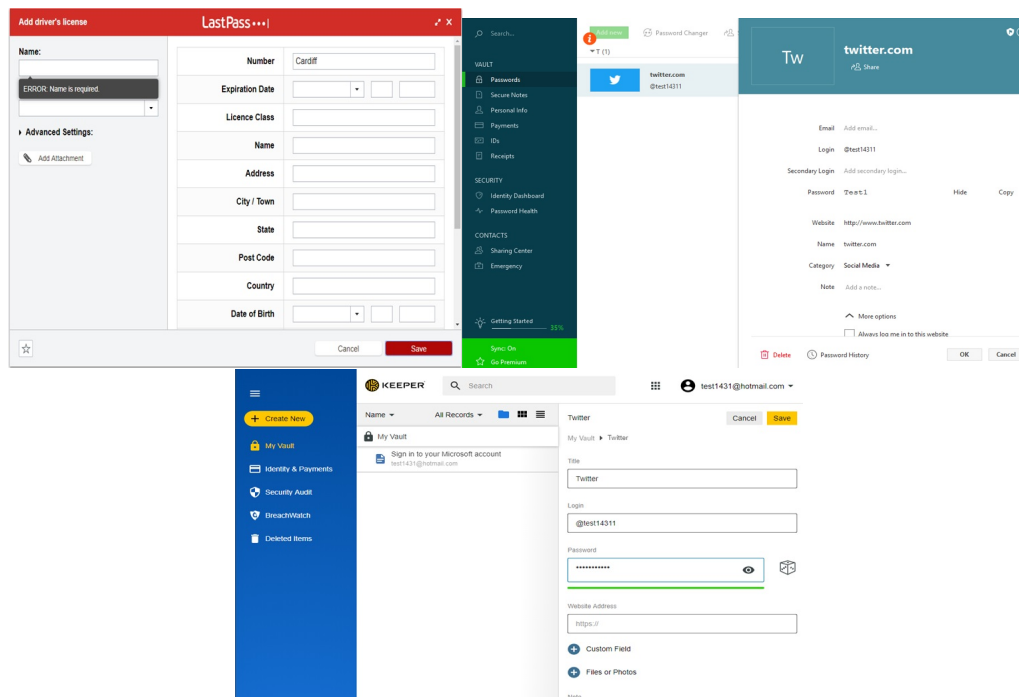


Figure 3.8: Data entry forms in LastPass, Dashlane and Keeper, which do not have asterisks. (Part of password in Dashlane is hidden).

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 novice and those with no computer science background. 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 action; for example, when a user wants to change a master password, a new page opens and says: “Set password” while the text says “Reset your LastPass master password”.

The recommendation to solve the problem is that the systems should consider all users and avoid using jargon, or provide explanation for the jargon on the page.

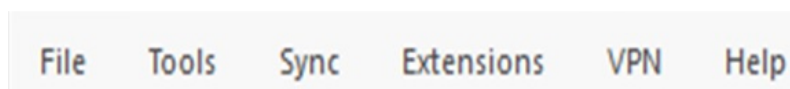


Figure 3.9: Computer jargon used in Dashlane (menu of Dashlane app)

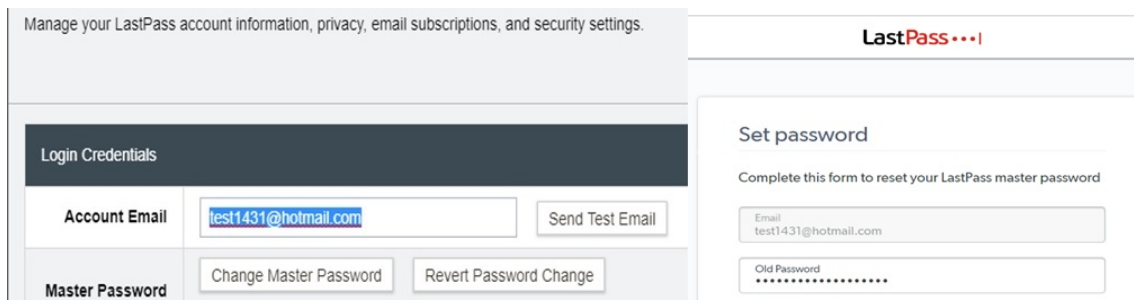


Figure 3.10: LastPass uses different words for the same action, change master password and set master password (no consistency).

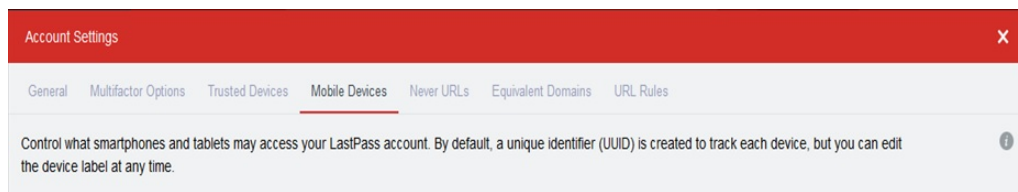


Figure 3.11: Computer jargon (account settings in LastPass).

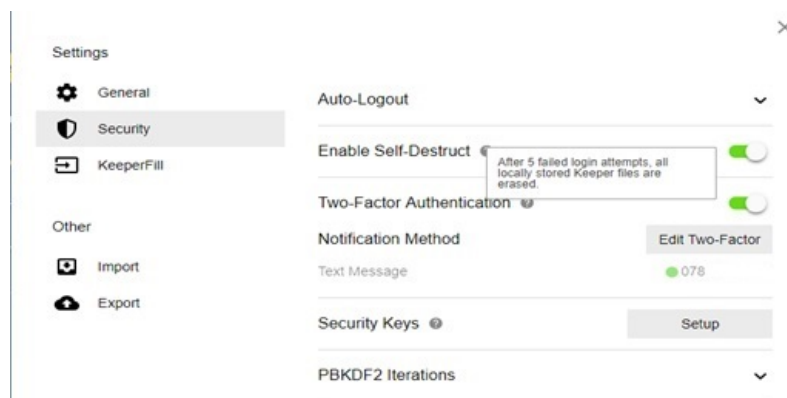


Figure 3.12: Computer jargon used in Keeper (part of phone number is hidden).

Account settings functions are not visible nor well organized in LastPass: This might not be acceptable to all users, especially when using grey colour. The colour of the account settings is not clear for all users.

The recommendation to solve this issue is that LastPass should use better and visible colours that suit all users.

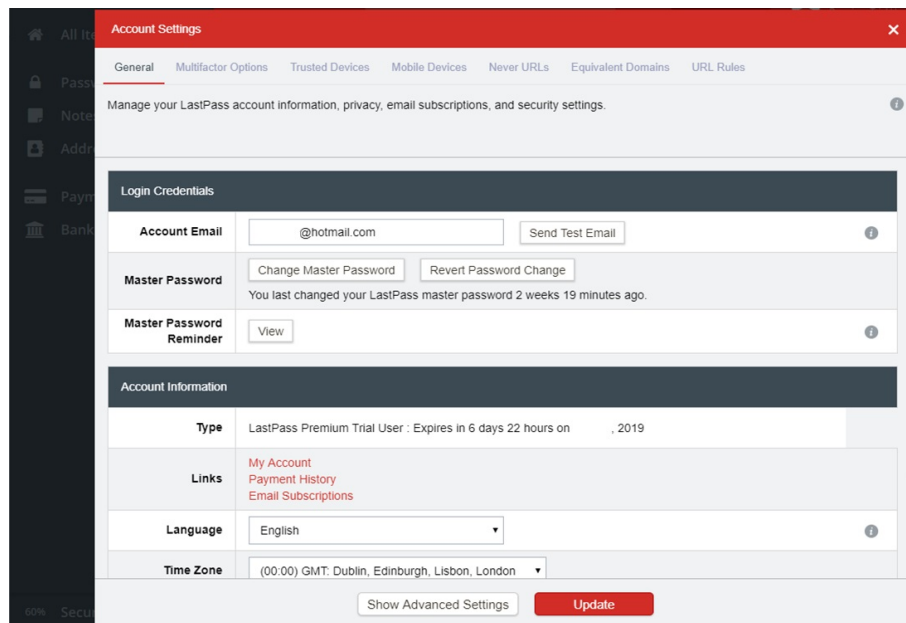


Figure 3.13: Colour of LastPass account settings. (Personal email and date are hidden).

Users can create a master password that does not match the requirements in 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.

The recommendation to solve the problem is that LastPass must use a stronger policy and prevent users from creating a master password that does not match the requirements.

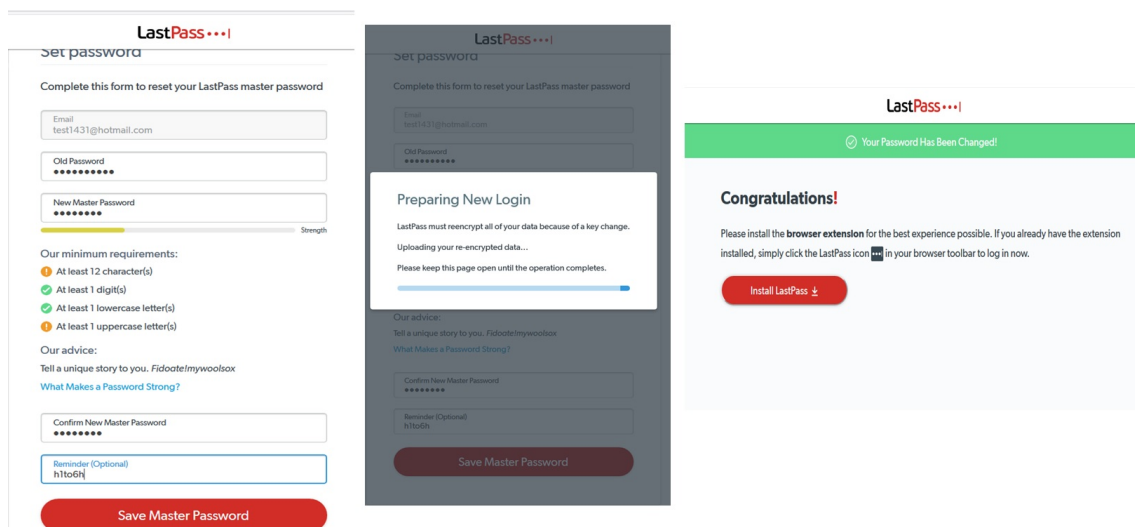


Figure 3.14: LastPass allows users to create a weak master password that does not match its policy.

Auto-change password does not work with websites and is not visible in LastPass:

This feature does not work for websites such as Twitter, it is not available for websites such as Hotmail, the button is not visible to all users because it looks like an error message.

The recommendation to solve the problem is that LastPass should show a list of websites for which passwords can be changed, similar to Dashlane's password manager. Also, the button of auto-change password should be clear and located in a better place.

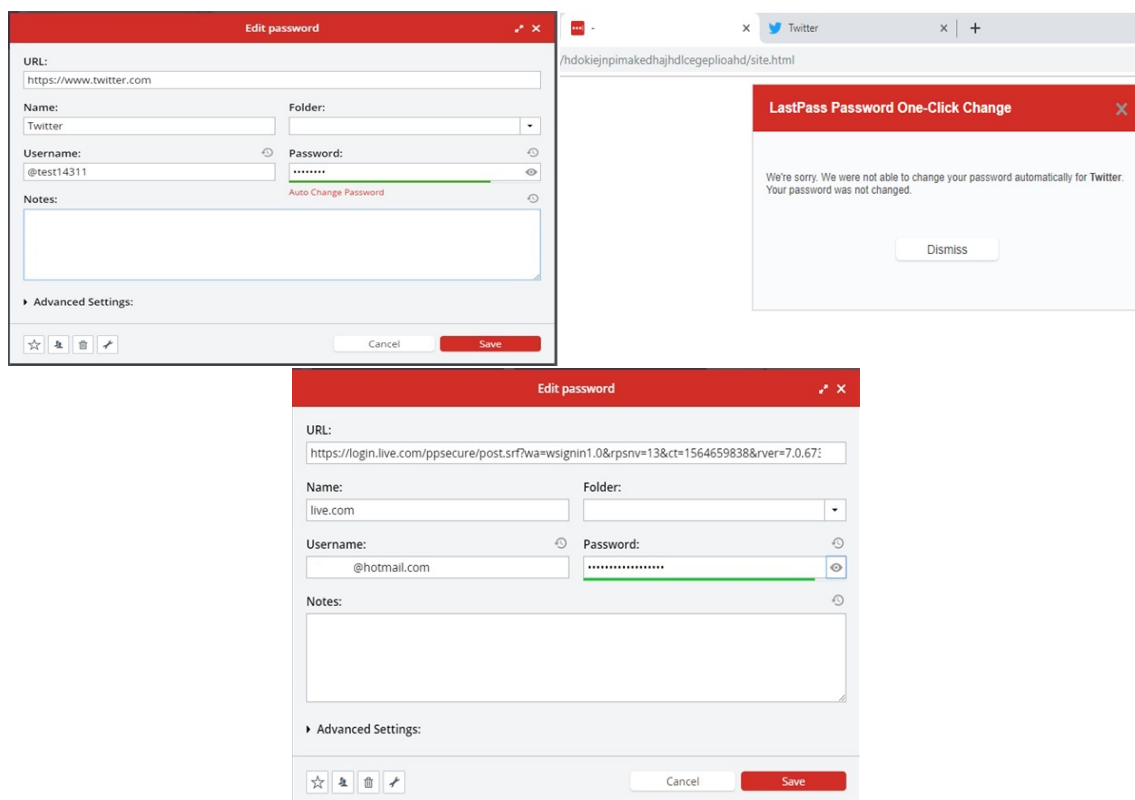


Figure 3.15: Auto-change password does not work in LastPass for Twitter. Also, it does not support all websites, for example, Hotmail. (Personal email is hidden).

Inconvenience when generating a new password in LastPass: Users have to figure out how to use the random password generator because there is a lack of instructions (e.g., copy password), it does not show the strength in words (only in colours), so novice users might find it inconvenient to use it to generate passwords.

The recommendation is that LastPass needs to label icons, also label passwords as weak and strong, which will be helpful for all users.

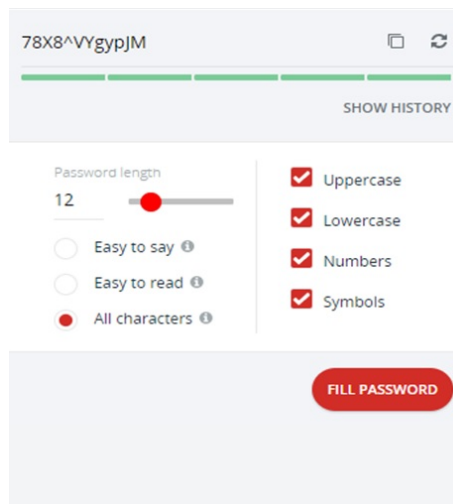


Figure 3.16: Random password generator for LastPass.

Recovering a LastPass account is difficult as it has to be from the same device and browser and requires authentication: If a user forgets the master password, they must use the same computer and the same browser that was used before with LastPass and install a browser extension, plus they have to use an authentication method (e.g., code to smartphone) for the recovery process; otherwise, the account will not be recovered and all data will be lost, except if the user uses emergency access.

The recommendation is that LastPass needs to alter the way users can recover an account to only using an authentication method, because using the device and browser that the user used before, and installing an extension, is a big restriction to complete the process of recovering an account.

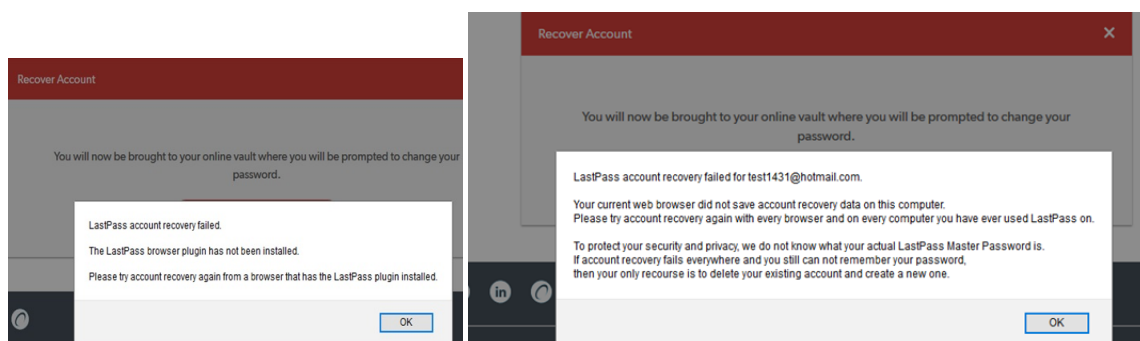


Figure 3.17: Very strict as users must use the same device and browser that was used before to recover and access LastPass account.

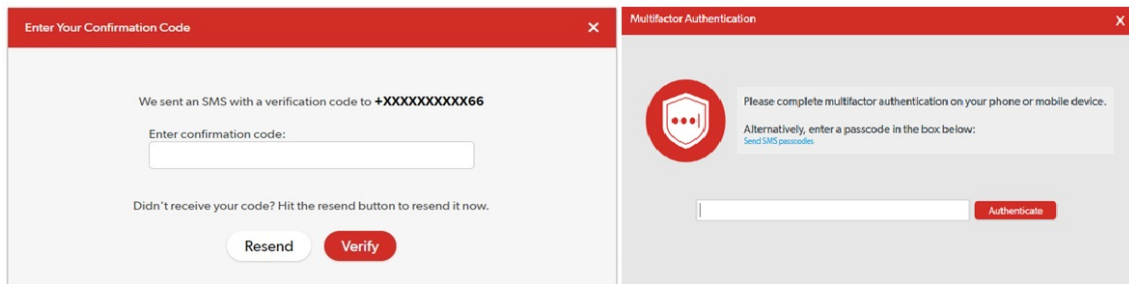


Figure 3.18: Required authentication such as SMS code, and authentication app such as LastPass authenticator app (if the app of Multifactor authentication is enabled).

Dark colours used for the main menu in Dashlane: This might not be liked by all users, especially when using dark colours for the menu and a small font.

The recommendation to solve the problem is that Dashlane should use better and brighter colours for the menu that suit all users.

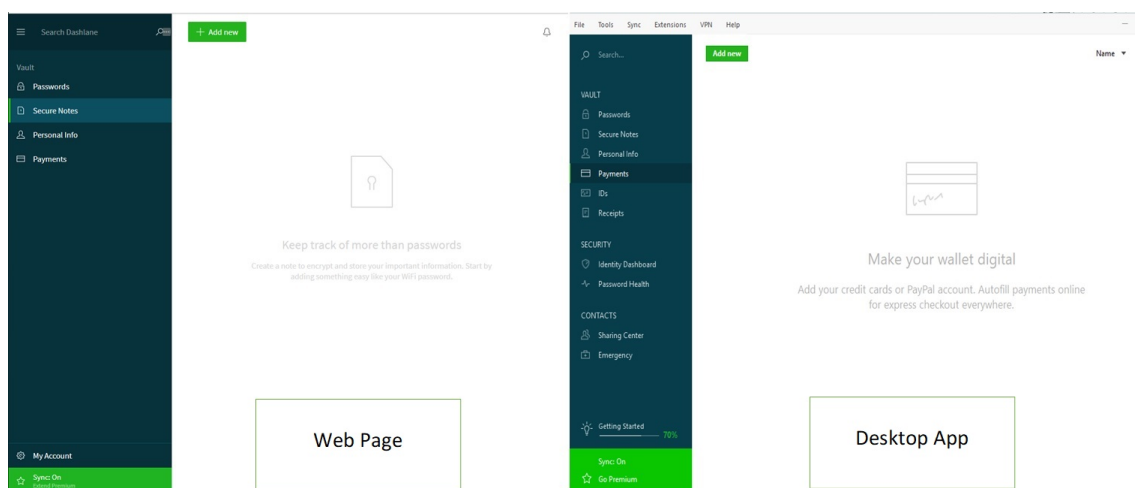


Figure 3.19: Colour of application and webpage of Dashlane.

Users can create a master password that meets strong requirements in Dashlane, but only by using an email address: 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 letter and adding a number.

The recommendation is that 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.

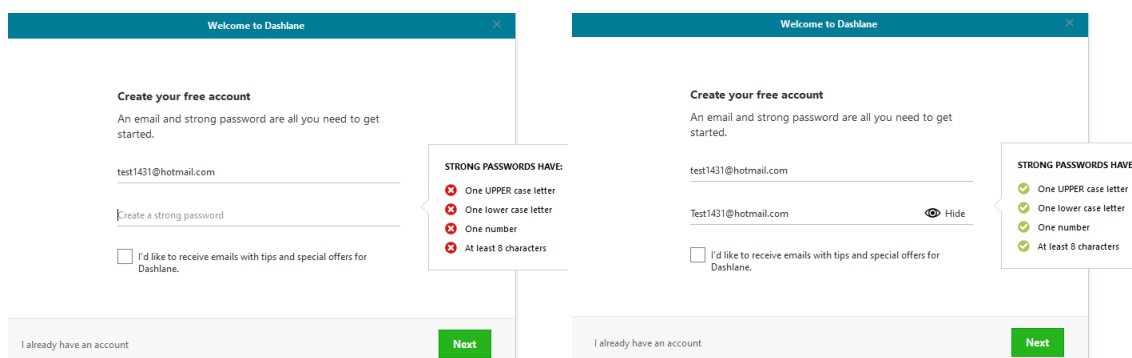


Figure 3.20: Users of Dashlane can create a master password using their email address.

Changing the master password in Dashlane while synchronization is disabled causes a loss of data stored on other devices: Users have to be careful when they want to reset the master password because if they do not have a premium membership and they change the master password, then all data stored on other devices will be lost. Dashlane shows an error message to warn users about the consequences.

The recommendation to solve the problem is that Dashlane should make this feature “free” for at least one extra device to encourage people to adopt it.

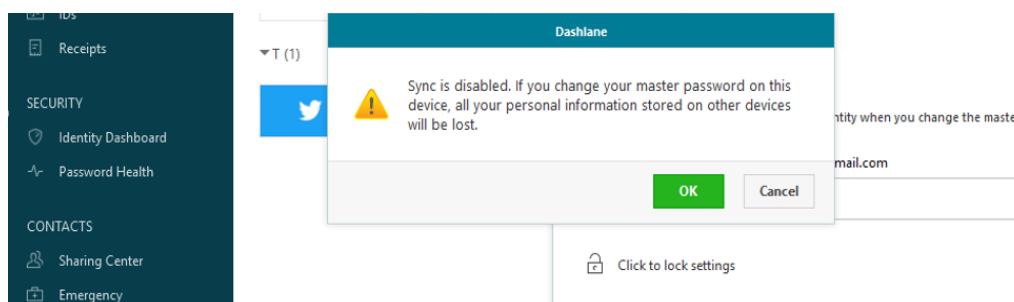


Figure 3.21: Changing the master password while synchronization is disabled causes a loss of data stored on other devices.

To recover an account in Dashlane, it requires contacting the business team and is “not free”: 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.

The recommendation is Dashlane should allow users of all devices to recover the account using authentication app, SMS code or sending a code to a registered email address.

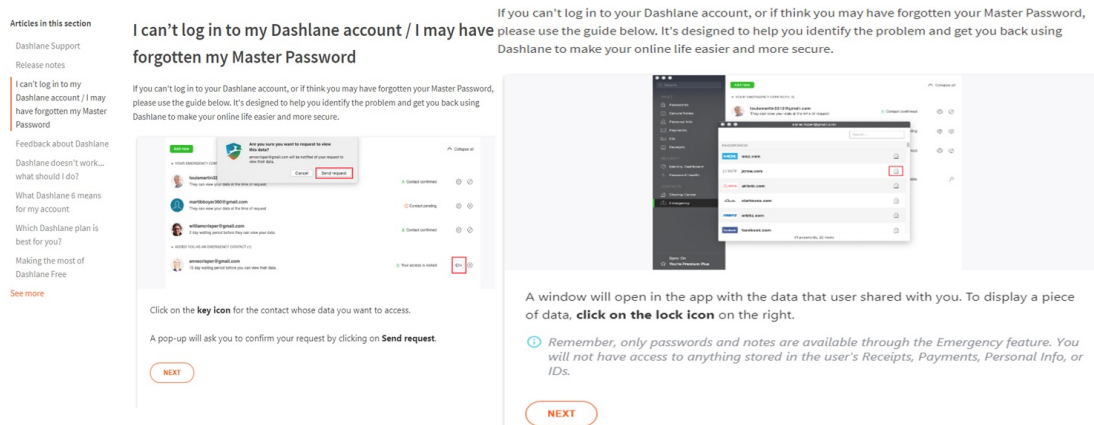


Figure 3.22: Recovering Dashlane account requires business team membership (not free).

Users have to install the Dashlane app to register and use all its functions and features, because it is not available on the webpage or in the browser extension: Users have to install Dashlane application to use specific features and functions because the webpage and browser extension do not have these features and functions.

The recommendation to solve the problem is that 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.

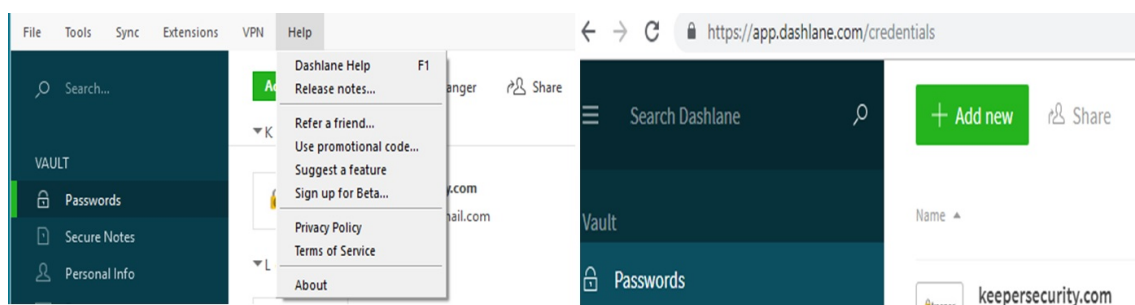


Figure 3.23: The application has all the features and functions, while the webpage does not.

Users can create a very weak master password in 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.

The recommendation to solve the problem is that Keeper must act and fix this as soon as possible by applying a strong master password policy and imposing it on all users.

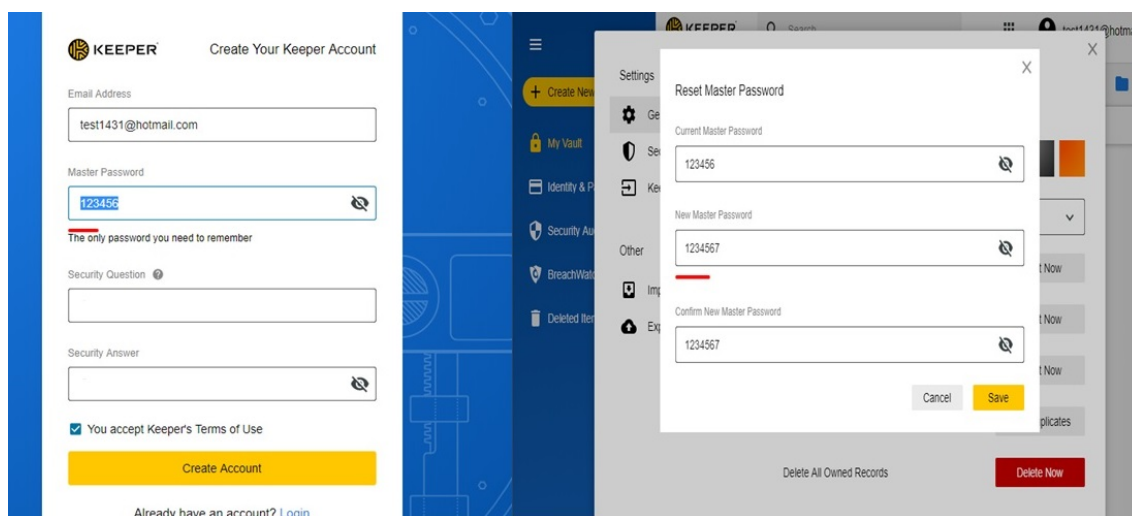


Figure 3.24: Keeper has a very weak policy for master passwords (the security question and answer are hidden in the left image.)

There is no random password generator in the browser extension of 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.

The recommendation to solve the problem is that Keeper needs to put a random password generator in the browser extension so it can be accessed easily by users.

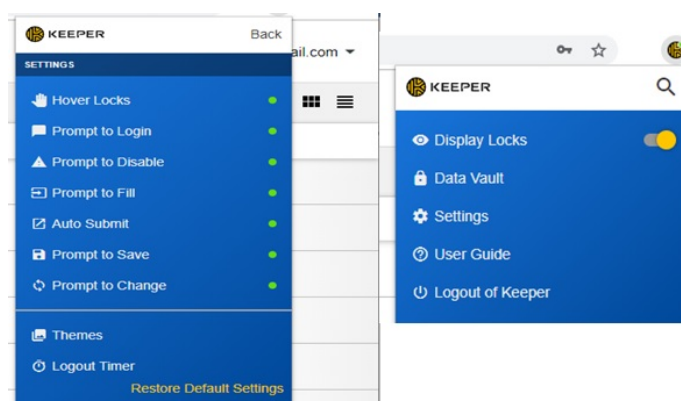


Figure 3.25: Keeper does not have a random password generator in the browser extension (an icon next to Keeper extension is hidden).

In the free version of Keeper, users can only use an application, but they cannot use a browser extension or webpage: This is an issue for normal users who do not have a membership because they can only use the Keeper application on the 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.

The recommendation is that Keeper should allow its users to use the browser extension and webpage for free on their device, and allow them to use an extra device for free.

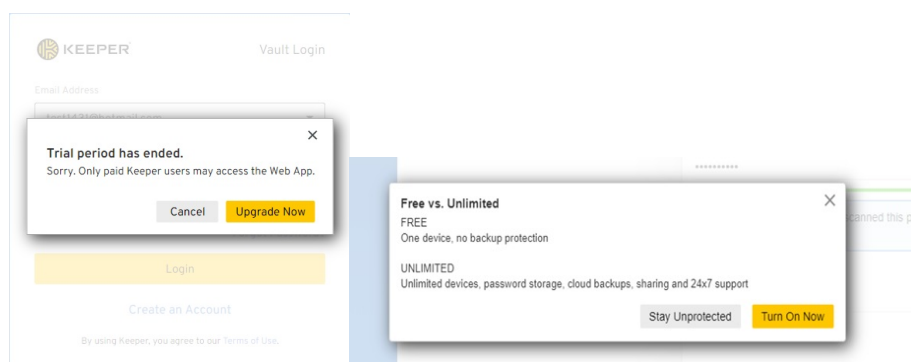


Figure 3.26: In Keeper, the webpage cannot be used on another device for free.

Old passwords are still stored in password managers: Old passwords that I had changed during the evaluation when I used 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 3.27: Old passwords stored in LastPass.

Table 3.6: A summary of the important problems that affect password managers.

- There is no undo function after saving new changes, so this should be fixed to help users to reverse wrong actions.
- Password managers should use terminology and language that familiar to users.
- Users must be prevented from inserting incorrect information such as invalid URL and email.
- Master password policy must be strong as well as password managers must not accept a master password if it does not match the requirements.
- In case a user forgets the master password, the process to recover the account should be flexible and easy.

3.4 Discussion

In this study of three cloud-based password managers (LastPass, Dashlane and Keeper), I found that they offer many useful features (Section 3.3.1, Table 3.4). 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 and they have consistent grammars and terminology.

They allow the user to copy and modify data, for example, the user can copy a password and paste it on the login 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 login form, thus the user does not need to remember them or type them which saves time. Regarding changing sensitive data, 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. The random password generator generates a random password once it is open and the user can change the length or remove characters. In LastPass and Dashlane password managers, users 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 the 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 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.

On the other hand, the three password managers have few problems that might affect their adoption by people (Section 3.3.2, Table 3.5). I found that there is no undo function when the user enters a master password and confirms an important change such as changing an email address or a master password. Also, there is no undo function if a user removes a username or password from account details and confirms the change. The three password managers do not prevent a user from inserting incorrect data in a field or storing incomplete data, for example, store an invalid 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 and those with no computer science background, for example, they use “vault”, “VPN” and “Breachwatch.”

Additionally, the three password managers do not have asterisks for mandatory field in data entry and dialog 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 is registered in Dashlane.

Significantly, recovering the account in LastPass is difficult as it has to be from the same device and browser that was used before and use an authentication method (e.g., smartphone app), while Dashlane requires contacting the business team which is not free, yet, android users can recover Dashlane account using their own biometrics. I also found that old passwords that I changed when using LastPass and Dashlane are already stored and not permanently deleted, which can be trust and transparency issues. So, users should be given an option to delete old passwords permanently.

3.5 Conclusion

This chapter investigated the user interface and usability of three popular cloud password managers and found that the usability and user interface design of these cloud-based password managers mostly satisfy Nielsen’s 10 principles, for example they have good design and offer useful features. However, they have some problems that violated Nielsen’s principles such as inserting incorrect data and using computer jargon, therefore, they need to

improve specific functions and features to make them suitable for all people to adopt.

In the next chapter of this research, I will look at the perspective of users and non-users of password managers. The aim is to investigate how users and non-users of password manager find it in different aspects such as usability and trust.

Chapter 4

User Study about Usability and Trust of Password Managers

4.1 Introduction

In the previous chapter, I investigated the user interface and usability of three cloud password managers and found that they mostly satisfied Nielsen's 10 principles, however, they have some problems that need to be solved. In this chapter, I looked at the human perspective regarding password managers. The aim of this study is to investigate and better understand how users and non-users of password managers find them in terms of usability and trust. Also, I want to understand the reasons why non-users refrain from using password managers. Thus, I conducted a user study with participants at Cardiff university, UK. The user study has two components, which are a usability test (user test) and an interview.

The results of the usability test (user test) show that most participants found it easy to access and store passwords in LastPass, while more than half of participants were satisfied with their experience and the language used. However, around half of participants found it difficult to recover the account and they found the design average. Also, I found no significant differences between users and non-users regarding ease of use and satisfaction of LastPass. In the interview section, the vast majority of participants would not trust the vendor to store all passwords or delete them permanently, and they would not let password

managers store bank and passport information. Likewise, half of participants do not know where passwords are stored, while most of them do not know the process.

4.2 Methodology

A user study which included a usability test (user test) and a semi-structured interview was conducted only with participants at Cardiff University, United Kingdom. Participants were recruited by sending emails to staff and students of school of computer science and to the representatives of other schools in the university, as well as distributing brochures. In total, 30 participants responded to our 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 (21 males and 9 females) and I estimate the age range to be between 24 and 45 years old.

Each participant completed the usability test using LastPass password manager, they did a number of tasks, 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 tasks in this study, the idea for the tasks comes from a pioneering study by Chiasson *et al.* [120] which were also applied in another study [77], [98]. The usability test has two new tasks (task 5 and 6) because LastPass has many features and functions within it. None of the participants were asked to use their own passwords or accounts. For the purposes of the study, username, email address, 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, the versions of LastPass used were between 4.31 and 4.36, but the change of versions did not affect the study at all, as the differences between LastPass versions are minimal and for the purpose of the study, these versions are equivalent. The interface of LastPass was configured to English and the whole study took around an hour 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 debriefing sheet after finishing the study which contains a thank you message, explains what will happen to the results and how they can contact us for further information. 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 (For all questions). I 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. I wrote down the participants' answers and comments during the usability test and interview while they answered usability questions. The questions were used as guidance.

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, from "1" very dissatisfied to "5" very satisfied, from poor to excellent and also open-ended questions. After participants answered the 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 study is to understand how users and non-users of password managers find it in terms of usability and trust, and investigate any similarities between users and non-users when they use a password manager, if LastPass is easy to use and password managers are trusted and to what extent users and non-users are knowledgeable about them.

Furthermore, the purpose for conducting a user test in-person with participants is that the user test is important, it helps the researcher to follow-up with participants while completing the tasks, and find out how easy or hard to use LastPass and its functions. Also, the user test is useful because the researcher can gather feedback from participants about the program, its design and functions. In regard to other methods of usability, I used inspection method (heuristic evaluation) in the previous chapter to evaluate the usability

and interface of three password managers. I did not consider using other methods such as eye tracking, because the aim was to test LastPass and its functions and gather answers and comments from participants about it, but not about participants' visual interactions with a page or which areas they focus on.

Moreover, the reason to have a face-to-face study and ask all participants to do the usability test using LastPass before the interview was to let them practise and use an actual password manager and test the usability in a monitored environment. So, they could understand the idea of password managers, how they work 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 I could elicit useful comments from them. 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 password managers, it can be used on multiple devices for free, it is free to use on the web page and browser extension with features and functions, and it provides an account recovery feature in case the master password is forgotten [107]–[114].

I conducted the usability tests and interviews until no new answers or comments emerged, I also had a good sample size from each group. Participants' comments were analyzed using inductive coding [121], which was used in study [86], where the codes were identified from the data. I read through the participants' comments, generated a set of codes, refined them and finalised them. For example, generating two different codes "multiple verification" and "higher security" from participants' comments, in which the final code for this is "security wise". Please note that the closed-ended questions which have numerical answers "Likert scale" were analyzed quantitatively and SPSS program was used for statistics, while open-ended questions and comments were analyzed using inductive coding. 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 [122],

while another study states that 10 users can reveal 80% of problems and 20 participants to reveal 95% of problems [123].

In the usability test, I compared users and non-users by using three factors: ease of use, satisfaction, effectiveness (Table 4.1). However, I did not use a standardized test such as System Usability Scale (SUS) to measure LastPass because the aim was to obtain answers about specific functions, which SUS does not offer. SUS is a set of 10 questions in 5 Likert scale (positive and negative questions) [124], [125], which covers different aspects such as training, support and complexity. 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 I had to ask these questions directly without using SUS. In fact, I obtained many comments from participants about the LastPass user interface and its functions, thus I obtained more details about LastPass and its user interface.

Table 4.1: 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.
Satisfaction	Design, language of the tool, overall experience and what is liked and least liked (disliked) by participants.
Effectiveness	Participant completes tasks accurately and successfully. (Did any participants not complete all tasks?) Which tasks could a participant not complete?

Seven tasks that were completed by participants in the usability test of LastPass
(All steps are in the appendix):

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 (steps 1,2,3).

Task 2 - Password migration: Participants store a password and an account for a website in LastPass (steps 4,5,6).

Task 3 - Login: Participants log in to the website where LastPass has already stored the account and password in task 2 (step 7).

Task 4 - Change password: Participants use the random password generator in LastPass to generate a new password, after that they change the password in the website. This task shows participants the security benefits of using a random password generator to generate a unique password for each account (steps 8,9,10).

Task 5 - Features discovery: Participants search for specific features in LastPass to enable/add, such as a 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 (steps 11 to 19).

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) (step 20).

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 (steps 21,22,23).

The aim of the user study is to discover if there are any similarities between users and non-users of password managers in terms of ease of use and satisfaction when using a LastPass password manager. In the interview part, 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. This study was reviewed and approved by the School of Computer Science Research Ethics Group, Cardiff University, UK.

4.3 Result

Before starting the usability test, I 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, while seven participants said they did not know anything about them. Surprisingly, I found that 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.

Table 4.2: Number of users and non-users of password managers.

Users	Non-users	Total of participants
16	14	30

I asked the 30 participants if they saved passwords in a web browser such as Chrome or Firefox, to ensure I could categorize them correctly later as users and non-users. I found that 16 participants were users of password managers and save passwords in a web browser (14 users used Chrome, one used Safari and another used LastPass). At the same time, two user participants who used Chrome said that they used Safari along with Keychain to save passwords. As for the other 14 participants, I found that some participants considered themselves non-users because they occasionally store some passwords or store a few unimportant accounts in a web browser and not use it mainly (the most used web browser was Chrome, followed by Firefox), while other non-user participants had never saved passwords in a web browser or any password manager program.

Thus, there were 16 participants who use a password manager to save passwords and considered themselves users, while 14 participants considered themselves non-users because they did not save passwords in any web browsers or password manager programs, or only store some passwords and a few unimportant accounts. Please note that 29 participants used LastPass 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 save and fill passwords.

4.3.1 Usability Test

As stated in the methodology section, I conducted a usability test (user test) using LastPass password manager because I wanted to see the participants use an actual example of a password manager, so that they would be able to clearly understand and answer the questions in this study (table 4.3). Also, I could then compare between users and non-users as regards a password manager (using specific functions) and explore their opinions about the tool, their design and language. As mentioned in the methodology, I compared users and non-users by using three factors which are ease of use, satisfaction and effectiveness.

1- Ease of use: Ease of using the system to complete tasks.

The findings show that the vast majority of participants (93%) agreed that it is easy to create an account in LastPass, while only two participants neither agreed nor disagreed. During the usability test, the 30 participants downloaded and installed the browser extension of LastPass (task 1); eighteen participants did not find it difficult to install the browser extension, while only four participants found it difficult. Also, 12 participants (40%) found it easy to use LastPass, while 14 participants (47%) answered neutrally. 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 found it difficult.

The 30 participants used the random password generator in LastPass to generate a random password for an online account and then changed it on the website (task 4), after that they should update it and then check the new password in the vault of LastPass. So, 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. Moreover, only one participant found

it hard to access stored passwords while 23 participants found it easy to access stored passwords in LastPass.

Table 4.3: 11 Statements were answered by 30 participants about using LastPass and specific functions.

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

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. The 30 participants used LastPass on two different devices (computers) while doing the usability test (task 7); 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 for the new device and the use of LastPass authentication app to let a new computer/device to be trusted on LastPass side. This task showed the participants how a password manager can be used on multiple devices and can synchronize passwords.

As the 30 participants 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. The actual fact is that LastPass uses “change” on the account settings page but “reset” on another page and it does not show the master password when it is typed. So, few participants said that LastPass uses two different words in the process of changing the master password which can be confusing, and LastPass should show the master password during the creation and changing stages.

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 using LastPass authenticator app and a smartphone to receive an SMS code (I provided a smartphone to all participants). Thirteen participants found it difficult to recover a LastPass account, while nine participants did not find it difficult. Few participants said that the account recovery is good and secure but paranoia and another machine should be used to recover the account. Finally, 11 participants (37%) would need help to be able to use LastPass, while nine (30%) disagreed.

To find out if there was any significant difference between 16 users and 14 non-users when using LastPass ($p < .05$), I used Mann Whitney test (non-parametric) to analyze the 11 usability questions because I have two different groups (users and non-users), and I do not have confidence in the normality of distribution. Please note that the questions and answers of (3, 5, 8, 10, 11) were inverted to positive during analysis in order to calculate the means and medians.

Table 4.4: The mean (average) and median, Mann Whitney U value and p-value of each usability statement for 16 users and 14 non-users (ease of use). For p-values, exact significance is displayed [2*(1-tailed sig.)].

	Statements	Mean & (Med.) of Users	Mean & (Med.) of Non-Users	Mann U Value	p-value .05
1	I find it easy to create an account in a password manager.	4.44 (4.50)	4.14 (4.0)	81.5	Not Sig $p = .208$
2	I find it easy to use a password manager	3.56 (3.50)	3.14 (3.0)	84.0	Not Sig $p = .257$
3	It is difficult to install the browser extension of a password manager. (inverted)	4.06 (4.0)	3.36 (3.0)	66.5	Not Sig $p = .058$
4	It is easy to store my online passwords in a password manager.	3.94 (4.0)	3.79 (4.0)	99.0	Not Sig $p = .608$
5	I find it hard to change my online passwords in a password manager. (inverted)	3.44 (3.50)	3.29 (3.0)	103.0	Not Sig $p = .728$
6	I find it easy to access my online passwords that are stored in a password manager.	4.0 (4.0)	4.07 (4.0)	110.0	Not Sig $p = .951$
7	It is easy to use a password manager on multiple devices.	3.50 (3.50)	3.0 (3.50)	90.0	Not Sig $p = .377$
8	It is hard to reset the master password. (inverted)	3.88 (4.0)	3.21 (3.0)	74.0	Not Sig $p = .120$
9	It is easy to find and use random password generator.	3.06 (3.0)	2.57 (3.0)	87.0	Not Sig $p = .313$
10	I find it difficult to recover my account if I forget my master password. (inverted)	2.50 (3.0)	2.93 (3.0)	89.5	Not Sig $p = .355$
11	I think I would need help/support to be able to use a password manager. (inverted)	3.06 (3.0)	2.43 (2.50)	78.0	Not Sig $p = .166$

* Please note that in the published paper [126], the mean (average) numbers are different by one because the range used in the paper is from 0 to 4, while the range used in this table is from 1 to 5.

As shown in Table 4.4, I found that more users found LastPass easy to use compared to non-users, but the difference between the two groups was not significant ($U = 84.0$, $p = .257$, $N = 30$). Also, users did not find it difficult to install the browser extension of LastPass compared to non-users, but the difference was not significant ($U = 66.5$, $p = .058$, $N = 30$).

Surprisingly, users found recovering a LastPass account more difficult compared to non-users; however, the difference was not significant between the two groups ($U = 89.5$, $p = .355$, $N = 30$). Similarly, non-user participants found it easy to access stored on-line passwords in LastPass compared to user participants, though the difference was not significant ($U = 110.0$, $p = .951$, $N = 30$). The results show that there were no significant differences between users and non-users of password managers when using LastPass password manager, which means that there are similarities between the two groups in their reporting experience for the 11 usability questions.

2- Satisfaction: Design, language, experience and what is most liked and disliked.

Furthermore, I asked the participants questions about their overall experience with LastPass, the language used and the design and layout (table 4.5), so I could measure their satisfaction. I found that 19 participants (63%) were satisfied with the overall experience, but four participants were very dissatisfied or dissatisfied. 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, 46% of participants found the design average, 27% participants found it fair while only 13% of participants rated the design as good.

Table 4.5: Three questions were answered by 30 participants about their satisfaction with using LastPass.

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

In order to find the differences between 16 users and 14 non-users, a Mann Whitney test was used to analyse the three satisfaction questions and p-values ($p < .05$). As shown in Table 4.6, 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 ($U = 94.0$, $p = .473$, $N = 30$). Users were more satisfied with the design and layout of LastPass compared to non-users, yet there was no significant difference between them ($U = 91.0$, $p = .400$, $N = 30$). The results show that there are similarities between users and non-users in the reporting of their experience of satisfaction.

Table 4.6: The mean (average) and median, Mann Whitney U value and p-value of each question for 16 users and 14 non-users (satisfaction). For p-values, exact significance is displayed [$2*(1\text{-tailed sig.})$].

	Questions	Mean & (Med.) of Users	Mean & (Med.) of Non-Users	Mann U Value	p-value .05
1	How would you describe your overall experience with a password manager?	3.63 (4.0)	3.29 (4.0)	94.0	Not Sig $p = .473$
2	How satisfied are you with the language used?	3.50 (4.0)	3.14 (3.50)	94.0	Not Sig $p = .473$
3	What are your thoughts on the design and layout?	3.06 (3.0)	2.64 (3.0)	91.0	Not Sig $p = .400$

* Please note that in the published paper [126], the mean (average) numbers are different by one because the range used in the paper is from 0 to 4, while the range used in this table is from 1 to 5.

In addition to the usability test about LastPass (above), I asked a further two questions about LastPass during the interview but added it to this section. So, 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 4.7). Notably, no non-users mentioned anything related to security. 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 4.7: Answers sample for the question “Most liked?”.

Code	Sample of answers
Save passwords (users)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Multiple factor authentication. • Security wise. • It has more security to protect data.
Auto-login (non-users)	<ul style="list-style-type: none"> • Allowing me to autologin. • Convenience in login to account. • Autologin.

3- Effectiveness: Participant completes tasks accurately and successfully.

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 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

The participants made many comments about LastPass. The comments from the participants reflected their opinions of LastPass, which may also apply to other cloud password managers. Participants found the design complex, not user friendly, and they have some security concerns (Table 4.8). However, some participants said LastPass provides good

security to protect account which is security wise. For example, participants said that the vault should open automatically, the menu is dark and not clear and there is no stars for mandatory field. Also, participants said what I am supposed to do if I do not have the smartphone and the adding icon should be under the bank icon in the menu.

Table 4.8: Comments sample about LastPass password manager.

Code	Comments
Complexity in design	<ul style="list-style-type: none"> • 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. • 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 menu. • The window setting has lots of options and not clear colour.
Not user friendly	<ul style="list-style-type: none"> • It should not ask me to install the extension again. • The name vault is not clear, it should be MySpace and so forth. • 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 wise	<ul style="list-style-type: none"> • 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.
Security concern	<ul style="list-style-type: none"> • Accessing and recovering account is strict. It should be flexible. • Easy to guess master password which is not good. • Master password should have a strong policy.
Good design	<ul style="list-style-type: none"> • It is good to have less items in menu and I can add what I want.

4.3.2 Interview Section

After finishing the usability test, I started the interviews (semi-structured) with 30 participants, asking them about their experience and about password managers in general, thus I could find out if there are similarities between the two groups in terms of trust in and knowledge about password managers.

The following questions were open-ended questions and the answers were analyzed qualitatively using inductive coding approach. Regarding the random generator, thirteen participants said they would expect to find a random password generator in account settings, five participants said they expected to find it in the password dialog box inside the vault, six participants said in the browser extension and five participants said on the main page of the password manager.

In case a password manager fails and passwords cannot be accessed; 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, I asked the 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, I asked non-user participants 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 the participants used LastPass, created and changed the master password during the usability test, I asked them how would you 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 user participant would use a hint to remember the master password. I also found that Windows is the most used by users (14), followed by Mac OS and Android (4 users), Linux (3 users) and iOS (2 users).

Closed-Ended Questions (Yes/No):

The next set of questions were (Yes/No) questions (Table 4.9), which were inspired by other studies in the literature such as [9], [40], [79], [83], reading news about passwords breach and own experience with password managers. I wanted to ask more questions because password managers are evolving. Password managers offer different features and they can store different types of important information, e.g., bank and passport details. Thus, I wanted to see if participants would let password managers store important information apart from storing passwords. The answers (Yes/No) were analyzed quantitatively (Table 4.9 and Figure 4.1), while participants' comments were analyzed qualitatively.

I asked 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 I intentionally made a weak master password "h1234567" for the usability test to find out if the participants would pay attention to its weakness. Twenty-four participants (14 users and 10 non-users) 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.

Table 4.9: Overall answers by 30 participants for (Yes/No) about password managers.

	Questions	Yes	No
1	Did you check the password strength when you created the master password?	24	6
2	Do you know what will happen if the master password is compromised/stolen?	28	2
3	Would you add an emergency contact to recover your account?	17	13
4	Do you know where a password manager stores passwords?	14	16
5	Do you understand how a password manager processes passwords?	9	21
6	Would you trust the browser extension of a password manager to fill in passwords?	19	11
7	Would you trust the vendor of a password manager to store all passwords?	5	25
8	Would you trust a password manager to delete password permanently from its database after you deleted it from vault?	5	25
9	Would you trust a password manager to retrieve account all the time?	27	3
10	Do you know that a password manager synchronizes passwords across devices using its own service?	28	2
11	Would you let a password manager store bank detail and passport information?	3	27
12	Would you install a browser extension of a password manager on a shared computer to access passwords?	2	28
13	Have you ever used a random password generator?	5	25
14	Do you know that Google Chrome and Firefox offer a built-in password generator?	5	25

Moreover, twenty-eight participants knew what would happen if the master password was compromised, while only two participants answered “No” (one user and one non-user). Participants stated that stored passwords would be accessed and compromised. Other participants suggested using multifactor authentication to accept the login or reject it, they would use two-factor authentication to prevent any login 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. Also, 17 participants (9 users and 8 non-users) checked the strength of Twitter password when they stored it in LastPass vault.

During the usability test, the participants came across a feature called “emergency access” 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 I asked the participants if they would add an emergency contact to recover the account, 17 participants said they would add an emergency contact (14 users and 3 non-users), while 13 participants said “No”.

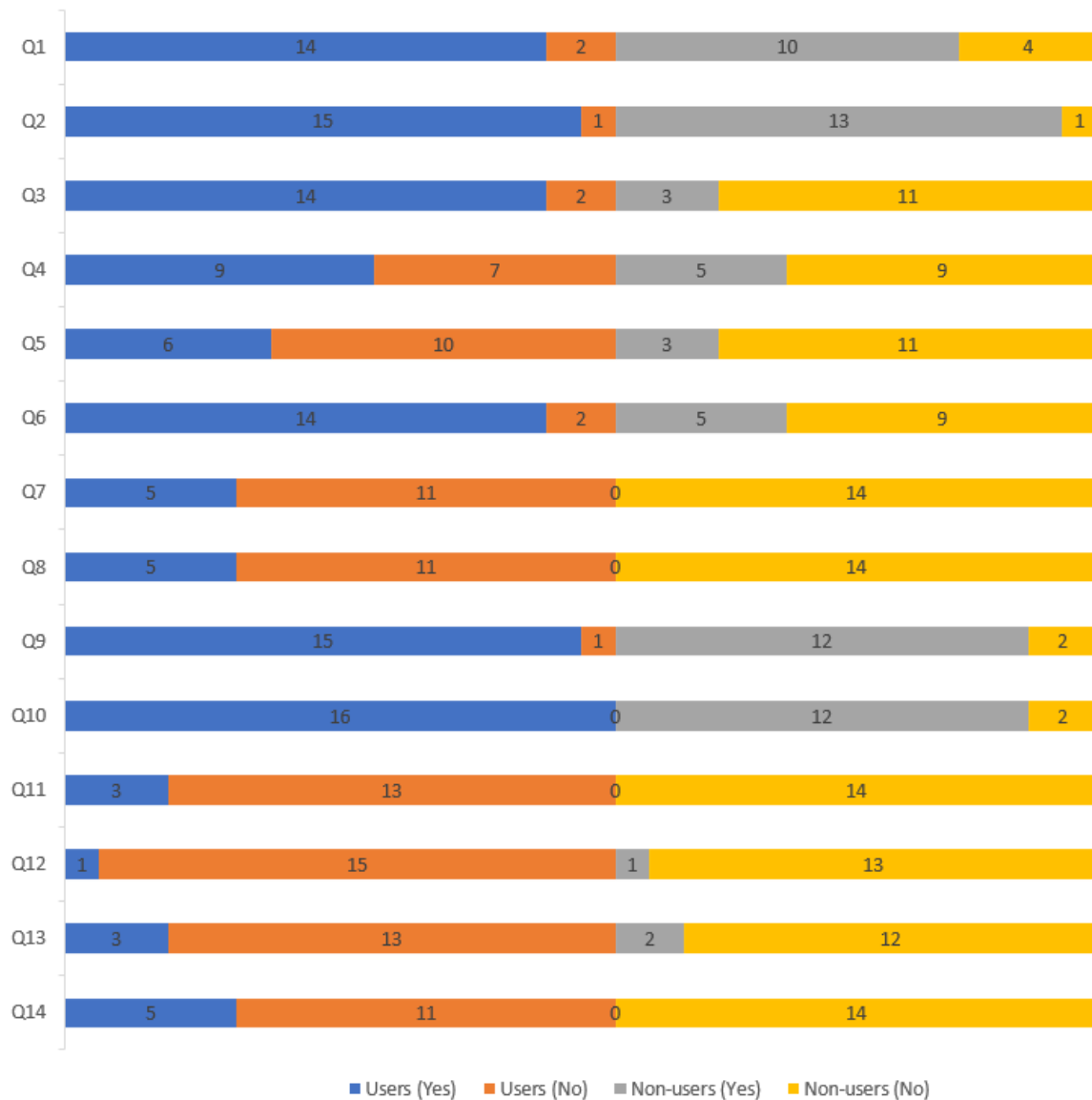


Figure 4.1: Answers by 16 users and 14 non-users for (Yes/No) questions about password managers and the similarities between the two groups.

Many participants gave some interesting reasons for not using this feature, for exam-

ple, they trust no one and 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, they would use it if it is free to add a personal account that belongs to them, and 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 answered 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. I 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 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.

Regarding the process in password managers, I found that most participants 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. Participants stated that passwords are stored 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. Few 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, 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 extension

with financial accounts, they would not use it for all websites, they would not trust it because somebody else might use the browser and they would not trust the computer.

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. Many participants said that they did not store bank passwords in a password manager, they cannot trust it particularly with important passwords and they do not know how password managers store passwords. 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 passwords but not with banking passwords. So, it can be seen that most of the comments are related to trust issues and security concerns (Table 4.10).

Table 4.10: Comments sample for the question “Trust the vendor of a password manager to store all passwords?”

Code	Sample of comments
Trust issue	<ul style="list-style-type: none"> • 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 prefer to remember my passwords. • I cannot trust them because they might access my accounts. • I have a trust issue if something happens to their server then it will be disaster. • I do not trust them.
Security concern	<ul style="list-style-type: none"> • 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.

I also found that 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 only store some passwords (not banking passwords), while only two users stored all passwords in a password manager that they are using. Furthermore, 27 participants would trust the password manager to retrieve account all the time, 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”. In regard to passwords synchronization, 28 participants knew that passwords are synchronized to other devices through password manager services.

Another finding is 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 towards password managers (Table 4.11).

Table 4.11: Comments sample for the question “Trust password managers to delete password permanently?”

Code	Sample of comments
Trust issue	<ul style="list-style-type: none"> • I do not trust them to delete my passwords. • I suspect they still have a copy of my password on offline storage. • They will keep the password even it appears to be deleted.
Transparency issue	<ul style="list-style-type: none"> • I do not know what they do with it. • I do not know what is happening in the other end.
Undeletable	<ul style="list-style-type: none"> • It is not possible to delete it technically because they have thousands of backups. • They cannot delete it, it is called digital footprint.

Moreover, 27 participants would not let password managers store bank details and passport information, while three users of password managers would store these details.

It implies that there are trust issues and security concerns towards password managers from both users and non-users. Three users who said they would let a password manager store these details 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.

In addition, 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 the comments, many participants said it is a shared computer, other people might access it and it is risky. Other participants said the machine might be compromised and it might have malware. Few participants stated that they might forget to log out, and passwords will remain once synchronization happens.

Regarding the use of a random password generator, only three users of password managers and 2 non-users used a random generator. Participants said that they cannot memorize passwords as they are difficult to remember and they do not know them (Table 4.12). Plus, only five users of a password manager knew about the built-in random password generators in Chrome and Firefox, while 11 users and 14 non-users did not know. This answer shows that users are more aware of built-in random password generator in web browsers than non-users. Regarding the comments, one participant said they never know, while another stated that they only knew about Chrome as a browser. Also, two participants who did not know about Chrome and Firefox said that they had seen a random generator in Safari web browser.

I asked users of password managers if they reuse the same password on multiple ac-

counts when they use a password manager. Shockingly, all users of password manager reuse passwords in multiple accounts or change some characters and use it. Also, a few users created weak (guessable) passwords. 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 a password manager fails to work. When I asked non-users if they reuse passwords, they 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”.

Table 4.12: Comments sample for the question “Have you ever used a random generator?”

Code	Sample of comments
Cannot memorize it	<ul style="list-style-type: none"> • 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.
Difficult to use	<ul style="list-style-type: none"> • I do not know how to use it. • I do not know how it works. • I cannot use it easily.
Trust issue	<ul style="list-style-type: none"> • I do not trust the generator and cannot remember. • I do not trust them.

Participants’ comments about password managers

At the end of the interviews, some user participants provided some comments about password managers and suggestions to improve it. One participant said it is enough to save passwords and share them between my devices, while another said it is better to store passwords on their own machine to have control of them. Also, other participants said that “people start using it now, but we need to know how to store it in the cloud”, “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 mentioned a few reasons that made them not to use password managers. Participants said that password manager is not safe to use, do not trust the software and cannot trust it to store passwords. Other participants said “I am afraid if my data is stolen, and I trust my memory”, “I trust my memory more than password manager” and “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 of password managers also said, “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”.

From the provided comments by users of password managers, it seems that password managers need to increase the security in order to protect users’ passwords and to gain their trust. Also, they should allow users to store passwords on their own device as well as improve the user interface to be more user friendly. Regarding the comments by non-users, it appears that they do not trust password managers, they view it as an unsafe tool to use or they do not care about it. Thus, password managers need to introduce itself to non-users as a useful and secure program, but first, password managers need to be more open and reassure non-users about stored passwords in the system.

4.4 Discussion

In the usability test part, I found that most of participants found it easy to access and store passwords in LastPass, found it easy to install browser extension, while 40% 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, therefore, LastPass should facilitate the way users recover the account in case they forget the master password.

Moreover, 46% of participants found the design and layout average which means LastPass should improve the design and layout. Participants liked saving and managing passwords the most, while users liked the security of LastPass. Also, participants did not like the design, colour, computer jargon and lack of flexibility as well as the way to access and recover the account is strict. Few participants stated things that are similar to the problems I found in LastPass in the previous chapter. They said that the account setting colour of LastPass should be better, no asterisks for mandatory fields, the use of computer jargon, recovering the account is strict and auto change password looks like an error sign. The vast majority of participants completed all tasks, and I found that there were no significant differences between users and non-users regarding “ease of use” and “satisfaction” of LastPass. Thus, users and non-users of password managers have similar experience in terms of ease of use and satisfaction when they use LastPass cloud password manager.

In the interview part, I found that user and non-user participants had similar knowledge of password managers as their answers about password managers are similar, particularly in terms of trust and transparency. The only differences I found are that most non-users do not want to add an emergency contact nor trust a browser extension to fill in passwords, whereas the majority of users do trust a browser extension and would add an emergency contact. Also, users trust password managers to store passwords, delete them

permanently and are more aware of built-in random password generator than non-users.

I found that most users used password managers mainly to save password and for easy access to accounts but the majority of them did not store all passwords. An interesting finding is that 28 participants knew the consequences if a master password is compromised which means that they know the importance of it, because compromising the master password means all passwords will be stolen. A few participants stated that the master password policy of LastPass is not strong and should have special characters. Also, 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.

Interestingly, the majority of users and all non-users would not trust password managers to store all their passwords or to delete passwords permanently from the databases, plus, they would not store bank and passport information in password managers. The results indicate 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. 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, I found that the great majority of non-users were aware of password synchronization in password managers and they trust password managers to retrieve their accounts all the time, which is similar to users of password managers. So, there are similarities in the reporting experience between users and non-users of password managers in many aspects such as trust and transparency.

Few participants made comments regarding password managers. They have trust issues towards the vendor of password managers because they do not trust it to store all passwords, and they think the programs are not safe which indicates a security concern. There is a lack of transparency towards password managers as participants do not know

if password managers delete passwords permanently and they do not know what they do with passwords. Other participants do not use password generator because the generated password is long and difficult to memorize, also, participants would not let password managers store bank and passport information due to security and trust issues.

4.5 Conclusion

In this chapter, I looked at the perspective of users and non-users of password managers. Most participants found it easy to create an account and store passwords in LastPass, as well as there were no significant differences between users and non-users regarding ease of use of LastPass. In the interview part, users and non-users of password managers have trust and transparency issues towards password managers as well as security concerns.

Finally, I extend the investigation about users and non-users of password managers using an online questionnaire (next chapter). I include the educational background to find out if education can play a role in using (or not using) password managers. The questionnaire will help to have more participants, different ages and education levels and explore more about users and non-users of password managers.

Chapter 5

Questionnaire Study about Users and Non-users of Password Managers

5.1 Introduction

In the user study (previous chapter), very interesting results were found such as users of password managers have many things in common with non-users regarding the usability of a cloud password manager as well as they have trust and transparency issues towards password managers. In this chapter, the investigation of the use and non-use of password managers was extended which also included educational background of participants.

In this study, I aim to find out if users of password managers, in big demographics, have trust and transparency issues and security concerns towards password managers as non-users, as well as if current password managers are easy to use for users and which functions are difficult to use, such as recovering a password manager account. Other aspects about users of password managers will be explored in this study such as storing all or some passwords, the use of a random password generator and which types of password managers are used the most (cloud-based, browser-based or open-source).

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 that are chosen by non-users. Is the low adoption of password managers related to trust issues, security concerns or other aspects? For the

definition of trust, transparency, security and adoption, please refer to chapter 1 (section 1.1). Trust and security are very important aspects in password managers, because password managers are expected to store passwords securely, in the meantime, users expect and trust password managers to store their passwords safely.

Moreover, the aim of this study is 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, the aim is to investigate whether there are any significant differences between expert and non-expert users in terms of many aspects such as trusting the vendors of password managers, and any security concerns towards password managers. Likewise, I want to find out if there are any significant differences between expert and non-expert non-users as regards to not using a password manager, for example, do not know how passwords are processed.

As for experts, the researchers [55] only consider 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 [57]. In this study, I 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, while those who have different educational background that is not related to computer science or information security are considered non-experts.

Furthermore, with more participants, different ages and different education levels, the questionnaire would provide a greater insight into issues such as trust, transparency and security for both users and non-users and allow to gather data from a large number of participants including experts and non-experts. Also, different aspects can be explored such as storing all passwords, the use of password generator and different types of password managers which could not have been done through the user study.

The results of this study show that trust is a big issue that makes non-users do not use a password manager, for example, they do not trust password managers to store pass-

words. It is followed by lack of transparency and security concerns, while usability is only a minor issue. Also, users of password managers have trust and transparency issues towards password managers along with security concern, and more than half of users do not store all passwords in password managers. However, users found it easy to use password managers as well as easy to store and access passwords. In regard to the educational background, there were significant differences between experts and non-experts in the number of accounts and passwords they have, however, having an education related to computer science or information security does not help to mitigate password reuse.

5.2 Methodology

I 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, e.g., using Chrome and LastPass), so I 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, I mapped each password manager to its user. Thus, the overall number of valid responses is 247.

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 and SPSS program was used for statistics, while open-ended questions were analyzed qualitatively using inductive coding approach. Different questions

for users and non-users of password managers were used because the aim is to understand their perspectives on using and not using password managers (For all questions). This study was reviewed and approved by the School of Computer Science Research Ethics Group, Cardiff University, UK.

5.3 Result

The online questionnaire was completed by 247 participants. I found that 22% were 18–25 years old, 43% of the respondents were 26–35 years old, 25% were 36–45 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 the participants varies, the majority of participants with a bachelor’s degree (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 that if participants’ educational background is related to 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, I 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 this study (table 5.1).

Table 5.1: Number of experts and non-experts in this study.

Experts	Non-Experts
128 (52%)	119 (48%)

As is known, companies and government sectors rely on the internet for various ser-

vices, 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. I found that 76 participants had more than 21 online accounts, followed by 51 participants with 11–15 accounts, and 37 participants had 16–20 accounts (Table 5.2). To find out if there was any significant difference between experts and non-experts, I used Chi-Square test. I found that there was a significant difference between experts and non-experts and the numbers of accounts they have $\chi^2(5, n=247) = 19.338, p < .002$.

Table 5.2: 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, I found that 137 participants had 1–5 passwords for their accounts, 31 participants had 21 or more passwords, 47 participants had 6–10 passwords and 14 participants did not know how many passwords they had. I compared between expert and non-expert participants regarding how many passwords they had to see which group had more passwords. As shown in Table 5.3, 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. I found that there was a significant difference between experts and non-experts and the numbers of passwords they have $\chi^2(5, n = 247) = 14.986, p < .010$. However, since 2 cells have expected value less than 5, I ran Monte Carlo and it shows similar result $p < .008$.

Table 5.3: 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

In order to see if there is any difference in regard to password reuse, the number of accounts and passwords were incorporated, but those who answered “I do not know” were excluded during the statistical test, because their answers do not indicate the number of accounts and passwords they have. For each participant, I compared the number of passwords (table 5.3) and number of accounts (table 5.2) they have in order to measure password reuse between experts and non-experts. The answer “1 to 5” is in range 1, the answer “6 to 10” is in range 2, the answer “11 to 15” is in range 3 and so forth. For example, if an expert has “16 to 20” accounts (range 4) and “1 to 5” passwords (range 1), this means this expert reuse passwords because they have more accounts than passwords and the new outcome of these two answers is 3 because $4 - 1 = 3$.

So, after incorporating the number of accounts and passwords for all participants, Mann Whitney test was performed because there are two different groups (experts and non-experts). The result shows that there was no evidence of differences between experts and non-experts regarding password reuse ($U = 5401.5$, $p = .341$, $N = 216$). Even though there were evidence in which experts have more accounts and passwords than non-experts, perhaps they do not have more passwords per accounts because when we look at the discrepancy between the number of passwords and number of accounts, there was no evidence of difference between experts and non-experts in regard to password reuse. Therefore, having an education related to computer science or information security does not play a significant role to mitigate passwords reuse.

Regarding the importance of accounts, 234 participants chose financial accounts as

very important accounts, 180 participants chose email accounts while 123 participants chose university/work accounts. Also, 100 participants chose shopping accounts while 94 participants chose social networks as very important.

The last question in this part is about the use of password managers. I asked the 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. I found that the number of expert non-users was 66 (52%), while expert users was 62 (48%). The number of non-expert non-users was 68 (57%), while non-expert users was 51 (43%) Table 5.4. To see if there was any significant difference between experts and non-experts in adopting password managers, a Pearson Chi-Square test was performed. I found that there was no significant difference between experts and non-experts in adopting a password manager $\chi^2 (1, n = 247) = 0.774, p = .379$. 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 5.4: Number of users and non-users, including experts and non-experts.

Experts	Non-Experts	Total of Users
62 (55%)	51 (45%)	113 (46%)
Experts	Non-Experts	Total of Non-Users
66 (49%)	68 (51%)	134 (54%)

Moreover, I intend to discover if there is any significant difference between users and non-users of password managers in the number of passwords and accounts they have (Table 5.5 and 5.6). Please note that the p-value of .000 is reported as .001 as suggested by [127], [128]. To see if there was any difference between the two groups, I used a Pearson Chi-Square test. The difference between users and non-users of password managers in the number of passwords was significant $\chi^2 (5, n = 247) = 28.172, p < .001$. However, since 2 cells have expected value less than 5, I ran Monte Carlo and it shows the same result $p < .001$. Likewise, I found a significant difference between users and non-users and the number of accounts they have $\chi^2 (5, n = 247) = 18.395, p < .002$.

Table 5.5: 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

Table 5.6: Number of accounts for 113 users and 134 non-users.

Online Accounts	Users	Non-Users
1 to 5	8	11
6 to 10	9	29
11 to 15	20	31
16 to 20	18	19
21 or more	48	28
I do not know	10	16

5.3.1 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 related to computer science or information security (non-experts), whereas 66 (49%) participants do have an educational background related to computer science or information security, so I 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 5.7) 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. Most of the reasons that were chosen related to trust issues, followed by security and transparency issues.

The reasons most selected by non-user participants related to trust issues, 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”. Also, 23.9% of participants chose “a password manager will not delete my password permanently from its database after I delete it from my account/vault”. 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 non-user 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 services.

Table 5.7: Number of times each reason was selected by 134 participants (66 experts and 68 non-experts), which also means these reasons were not selected by the remaining participants. It shows the overall time and percentage of reasons selected by both groups. Note: numbers do not add up to 100% as participants could choose more than one reason.

	Reasons	Experts	Non-Experts	Overall
1	I find it difficult to use a password manager.	6	14	20 (14.9%)
2	It is hard to update my passwords.	1	6	7 (5.2%)
3	It is difficult to recover my account if I forget my master password.	12	12	24 (17.9%)
4	I do not trust the browser extension of a password manager to fill in my passwords.	30	26	56 (41.8%)
5	I do not trust the vendor of a password manager to store my passwords.	38	18	56 (41.8%)
6	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%)
7	My passwords will be synchronized to my other devices using the vendor's services.	14	13	27 (20.1%)
8	I do not know where my passwords will be stored in a password manager.	28	23	51 (38.1%)
9	I do not know how my online passwords will be processed in a password manager.	15	15	30 (22.4%)
10	All my passwords will be leaked if the database of a password manager is hacked.	30	18	48 (35.8%)
11	If my master password is compromised/stolen, all my passwords will be exposed.	19	16	35 (26.1%)
12	People who use my computer will be able to login to my password manager.	14	19	33 (24.6%)
13	If a password manager fails to work, I will not be able to retrieve my online passwords.	23	16	39 (29.1%)

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 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%).

Importantly, the last reasons chosen by non-user participants from the list are related to usability, as only 14.9% chose “I find it difficult to use a password manager”, 17.9% selected “it is difficult to recover the account if I forget the master password” while 5.2% found it hard to update passwords in a password manager. These results show that non-user participants do 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 towards 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 non-users are related to trust when compared to security and transparency, while reasons related to usability were chosen least by non-users (experts and non-experts). Thus, I identified the reasons for the low adoption rate of password managers in numbers and percentages.

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), I performed an analysis using a Pearson Chi-Square test (Table 5.8). I 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 .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 $\chi^2 (1, n = 134) = 0.718, p = .397$.

Table 5.8: 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	Chi Value	p-value .05
1	I find it difficult to use a password manager.	3.487	Not Sig $p = .062$
2	It is hard to update my passwords.	3.613	Not Sig $p = .057$
3	It is difficult to recover my account if I forget my master password.	.007	Not Sig $p = .936$
4	I do not trust the browser extension of a password manager to fill in my passwords.	.718	Not Sig $p = .397$
5	I do not trust the vendor of a password manager to store my passwords.	13.321	Sig $p < .001$
6	A password manager will not delete my password permanently from its database after I delete it from my account/vault.	.823	Not Sig $p = .364$
7	My passwords will be synchronized to my other devices using the vendor's services.	.091	Not Sig $p = .763$
8	I do not know where my passwords will be stored in a password manager.	1.051	Not Sig $p = .305$
9	I do not know how my online passwords will be processed in a password manager.	.009	Not Sig $p = .926$
10	All my passwords will be leaked if the database of a password manager is hacked.	5.250	Sig $p < .022$
11	If my master password is compromised/stolen, all my passwords will be exposed.	.480	Not Sig $p = .488$
12	People who use my computer will be able to login to my password manager.	.817	Not Sig $p = .366$
13	If a password manager fails to work, I will not be able to retrieve my online passwords.	2.080	Not Sig $p = .149$

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 $\chi^2 (1, n = 134) = 13.321, p < .001$. 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 $\chi^2 (1, n = 134) = 5.250, p < .022$.

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. Please note that option 2 “hard to update my passwords” has an expected value that less than 5, so its Fisher exact test is $p = .115$

In addition, to see which category was selected the most by non-user participants, every three reasons were grouped into a category (Table 5.9) 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 not counted by McNemar (table 5.10), 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 5.9: Every three reasons from Table 5.8 were grouped in a category. McNemar test was used to see if there was any significant difference between these categories.

Usability Category
<ul style="list-style-type: none"> • I find it difficult to use a password manager. • It is hard to update my passwords in a password manager. • It is difficult to recover my account if I forget my master password.
Trust Category
<ul style="list-style-type: none"> • I do not trust the browser extension of a password manager to fill in my passwords. • I do not trust the 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
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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 $< .001$ and test statistic = 26.30. (61 non-user participants chose only trust reasons and 16 non-users only chose usability reasons, 25 non-users who chose from both categories were excluded, while 32 non-users 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 $< .001$ and test statistic = 14.06 (47 non-users chose only transparency reasons, 17 chose only usability, 24 non-users who chose from both categories were excluded, while 46 non-users 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 $< .001$ and test statistic = 14.78 (48 non-users chose only security reasons, 17 non-users chose only usability reasons, 24 non-users who chose from both categories were excluded, while 45 non-users did not choose from security or usability category). The findings show that usability is not the main reason for not using a password manager, rather it is the trust issue followed by transparency and security.

Table 5.10: Comparing between 4 categories that were selected/not selected by 134 non-users. McNemar test was used to find the significant difference between the categories.

Usability	Trust	Both chosen	Not chosen	p-value .05
16	61	25	32	Sig $p < .001$
Usability	Transparency	Both chosen	Not chosen	p-value .05
17	47	24	46	Sig $p < .001$
Usability	Security	Both chosen	Not chosen	p-value .05
17	48	24	45	Sig $p < .001$
Trust	Transparency	Both chosen	Not chosen	p-value .05
36	21	50	27	Not Sig $p = .063$
Trust	Security	Both chosen	Not chosen	p-value .05
31	17	55	31	Not Sig $p = .059$
Security	Transparency	Both chosen	Not chosen	p-value .05
24	23	48	39	Not Sig $p = 1.0$

I also performed a McNemar test to see if there was any significant difference between the trust, transparency and security categories. I found no significant differences between the trust, transparency and security categories as the McNemar exact p -value was greater than .05. There was no significant difference between the trust and trans-

parency categories as shown by the McNemar exact p -value = .063 and test statistic = 3.947 (36 non-users chose only trust reasons, 21 chose only transparency, 50 non-users who chose from both categories were excluded, while 27 non-users did not choose from transparency or trust category). There was no significant difference between trust and security categories as McNemar exact p -value = .059 and test statistic = 4.083 (31 non-users chose only trust reasons, 17 chose only security, 55 non-users who chose from both categories were excluded, while 31 non-users 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 non-users chose only security reasons, 23 chose only transparency, 48 non-users who chose from both categories were excluded, while 39 non-users did not choose from transparency or security category).

As seen above, when I compare between the four categories, I found that the most selected category is trust which implies that there are some indications that trust is more important obstacle for not using password manager, followed by transparency and security categories as both categories have a similar number of selected times, yet, they were not selected as many times as trust category. Also, I found that fewer non-user participants selected usability category when compared with trust, transparency and security categories, therefore I can see that usability is only a minor issue for non-users. Moreover, I found that the difference between usability category and the other three categories (trust, transparency and security) is significant. However, there was no significant difference between trust, transparency and security categories, yet, trust was selected the most by non-users.

A number of non-user participants made 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.

5.3.2 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 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, 24% are between the ages of 18 and 25 years, 46% of users are aged 26–35 years and 20% are 36–45 years old.

The results show that 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 (Table 5.11). 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 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 5.11, 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 5.11: Types of password managers used by 113 users (62 experts, 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/iCloud 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%)

I also found that 58% of users do not store all their passwords, while 42% of 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 5.12), I 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, I used a Pearson Chi-Square test. I found that there was no significant difference between experts and non-experts in storing passwords in password managers $\chi^2(1, n = 113) = 0.720, p = .396$.

Table 5.12: 62 experts and 51 non-experts (113 users) who store all or some passwords.

	Experts	Non-Experts	Total
Store all passwords	28 (60%)	19 (40%)	47 (42%)
Store some passwords	34 (52%)	32 (48%)	66 (58%)

To find out in which password managers users store all their passwords, I 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. For LastPass, 11 (48%) users store all their passwords, 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.

Furthermore, 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 (Table 5.13). This finding shows that half of the users do not use a random password generator for each account although it is offered within the tool. In regard to experts and non-experts, I 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, I found that no significant difference between experts and non-experts as regards using a random password generator $\chi^2 (2, n = 113) = 2.682, p = .262$.

Table 5.13: 62 experts and 51 non-experts (113 users) who use a password generator.

Using Random Generator	Experts	Non-Experts	Total
Use it for each account	22 (67%)	11 (33%)	33 (29%)
Use it only for specific account	12 (52%)	11 (48%)	23 (20%)
Do not use random generator	28 (49%)	29 (51%)	57 (51%)

In detail, I 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 might 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, participants who do not use a random password generator an-

answered another question about the reason that applied to them; 42% did not know that a password manager offers a built-in random password generator, while 19% of users did not know how to use a random password generator. Other users reported many different reasons, 19% said it is hard and complex to remember, 7% prefer to create passwords by themselves that are memorable, while others said in case I cannot access the manager. Also, other users said that they never thought about it, do not feel safe and do not need it.

Most users heard of password managers from social media, followed by advertisement, IT magazine/article and family/friends. Other respondents said they heard of a password manager from YouTube, antivirus recommendation and suggested by browser, e.g., Chrome. Also, 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), while 20% of users said they forgot the master password.

Moreover, I asked the user participants an open-ended question “Why are you using a password manager?” and analyzed it qualitatively using inductive coding (Table 5.14). Participants’ answers were analyzed using inductive coding, where the codes were identified from the data. I read through the participants’ answers, generated a set of codes, refined them and finalised them. I found that 46% of users use password managers to store passwords because they cannot remember all of them, 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, while 7% said to generate a unique password for each account and to avoid reuse.

Table 5.14: Answers sample for “Why are you using a password manager?”. Frequencies of codes being applied to participants’ reasons for using password managers. Please note that numbers add up to 100%. Participants could have one or more reasons in one answer.

Frequencies	Code	Sample of answers
46%	Store passwords as they cannot be remembered	<ul style="list-style-type: none"> • To store passwords. • To help me to remember. • Because I can’t remember all my passwords. • Because I always forget my password. • To keep track of my passwords. • To aid remembering unique passwords and to keep records of logins and urls. • It is difficult to memorize many passwords. • Saves me from having to remember or write down all of my passwords. • Cause I forget my password many times.
26%	Easy to login and fast access	<ul style="list-style-type: none"> • Easy to access. • Makes my life easier to log in to everything. • It’s quicker to log into all the things I use regularly. • So that I don’t have to type it every time. • Easy and have auto save. • To get fast access to my password as I needed.
17%	Security and protection	<ul style="list-style-type: none"> • Protect my account. • Keep all passwords securely in one place. • To secure my accounts. • Security, different password per account and convenience.
7%	Generate unique password and avoid reuse	<ul style="list-style-type: none"> • To ensure that I do not reuse passwords for sites. • To generate a strong and long password. • Too many websites, can’t remember password for all 100+ websites I may use, want to use complex passwords for each.

Usability of Password Managers:

To find out how easy it is to use password managers and their functions, I asked the user participants to answer 10 questions about password managers (table 5.16). 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, I analyzed different password managers which are browser-based (Chrome), cloud-based (LastPass, Dashlane, 1Password) and open source (KeePass) in Table 5.15.

Table 5.15: Analyzing 5 different password managers (number of users for each program).

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

I found that all users of LastPass, Dashlane and KeePass and nine users of 1Password found it easy to create an account. Likewise, all users of KeePass, Dashlane and 1Password and 22 users of LastPass found it easy to store online passwords. In addition, all users of KeePass, Dashlane, 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, and also, easy to store passwords.

As for installing the browser extensions of LastPass, Dashlane, 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, Dashlane, KeePass and all 1Password users found it easy to access their online passwords. Similarly, only one user of Dashlane and two users of LastPass need help to use the program. Furthermore, most users of LastPass, 1Password and KeePass and 2 Dashlane users found it easy to change passwords, but a few users found it hard to change.

When I asked these users about using password managers on multiple devices, 14

users of LastPass, seven users of 1Password, two users of Dashlane and two users of KeePass found it easy to use the programs on multiple devices. However, a few users of LastPass, Dashlane and KeePass found it difficult to use the programs on multiple devices. Also, eight users of LastPass, one user of Dashlane, 1Password and KeePass found it hard to reset the master password. But a few users chose “not applicable”, 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. The result is that seven LastPass users, five 1Password users, 4 Dashlane 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, KeePass and Dashlane chose “not applicable”, which means they have never forgotten their master password or have never tried to recover their account, or perhaps they do not know how difficult it is. It appears that password managers are easy to use and easy to store passwords and access them, but they still have issues regarding their use on multiple devices and recovering accounts.

With regard to 52 Chrome users, I found that the great majority of users found it easy to use Chrome (89%) and easy to store passwords (82%). Similarly, 67% of Chrome users found it easy to use on multiple devices, while only 12% did not find it easy. Moreover, 73% of users found it easy to create an account, while only 23% found it difficult to install the browser extension. 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. These results indicate that Chrome is well-known and accessible. However, only 31% of Chrome users found it easy to change their passwords, 34% neither agreed nor disagreed, while 29% found it hard to change passwords in Chrome.

Lastly, 31% of Chrome users found it hard to reset the master password, and only 21% would need help to use it. Regarding recovering the account, 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 [129]. 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.

Table 5.16: 10 Usability statements were answered by users of password managers.

	Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	I find it easy to create an account in a password manager.	35%	49%	10%	2%	0%
2	I find it easy to use a password manager.	37%	54%	7%	1%	1%
3	It is difficult to install the browser extension of a password manager.	5%	12%	19%	28%	24%
4	It is easy to store my on-line passwords in a password manager.	41%	50%	7%	2%	0%
5	I find it hard to change my on-line passwords in a password manager.	7%	18%	22%	27%	18%
6	I find it easy to access my on-line passwords that are stored in a password manager.	25%	55%	13%	3%	4%
7	It is easy to use a password manager on multiple devices.	24%	42%	19%	11%	1%
8	It is hard to reset the master password.	7%	18%	32%	19%	7%
9	I find it difficult to recover my account if I forget my master password.	20%	21%	19%	11%	6%
10	I think I would need help/support to be able to use a password manager.	4%	11%	20%	22%	40%

* A few users answered (N/A) to question 1 (4%), question 3 (12%), question 5 (8%), question 7 (3%), question 8 (17%), question 9 (23%) and question 10 (3%).

Trust and Security of Password Managers:

Previous studies on password managers did not primarily focus on the view of users of password managers and stored passwords. In this study, I believe that there are many users of password managers who have trust and transparency issues and security concerns towards password managers (Table 5.17). Also, I 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 (Table 5.18). Please note that I used a Mann Whitney (non-parametric) test to check for any significant difference between two different groups (experts and non-experts).

First, I asked user participants if they knew where passwords are stored in a password manager; the findings show 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. I 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 know about the location of stored passwords.

Similarly, 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, I 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.

I also found that 65% felt confident to use a browser extension to fill in passwords, while 10% did not feel confident to do so. However, three non-expert users chose “not applicable” (one Chrome, one Firefox, one Safari user). The 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. Likewise, 72% of users were aware of password synchronization using a vendor’s service, while only 9% were not aware. I 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. I 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, I 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, I found that half of users of Chrome, LastPass, 1Password and more users of Safari and Dashlane were worried about losing their stored passwords 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.

Table 5.17: 12 Statements were answered by 113 users about password managers.

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

* A few users answered (N/A) to questions 3 and 9 (3%), question 10 (4%), question 12 (2%).

Additionally, 47% of users trust password managers to delete their passwords permanently from their databases, while 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 password managers either do not trust them or are not sure if their passwords will be deleted.

When I asked the 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, I 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. I found that 46% would not let a password manager store bank details and passport information, 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, I analyzed them individually. Most LastPass and Chrome users would not store their personal information, while no Dashlane users would store their information. On the other hand, eight 1Password users and all KeePass users would store this information.

Looking at Table 5.18, I 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 .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 ($U = 1544.0$, $p = .826$, $N = 113$). Similarly, there was no significant difference between experts and non-experts in terms of trusting vendors to store all their passwords ($U = 1491.5$, $p = .590$, $N = 113$).

As seen in table 5.18, 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 from the database and are aware of password synchronization compared to non-experts. However, the differences between expert and non-expert users are not significant for using password managers. Therefore, having an education related to computer science or information security does not play any important role in using password managers.

Table 5.18: Comparing 62 experts and 51 non-experts regarding using password managers. The mean (average) and median, Mann Whitney U and p-value of each statement.

	Statements	Mean & (Med.) of Experts	Mean & (Med.) of Non-Experts	Mann U Value	p-value .05
1	I know where my online passwords have been stored in a password manager.	3.26 (3.0)	3.33 (4.0)	1544.0	Not Sig $p = .826$
2	I fully understand how a password manager processes my online passwords.	3.02 (3.0)	3.08 (3.0)	1538.5	Not Sig $p = .800$
3	I feel confident to use browser extension of a password manager to fill in my passwords.	3.76 (4.0)	3.60 (4.0)	1354.5	Not Sig $p = .390$
4	I trust the vendor of a password manager to store all my online passwords including my sensitive passwords.	3.24 (3.50)	3.39 (4.0)	1491.5	Not Sig $p = .590$
5	I worry about losing all my passwords that are stored in a password manager.	3.42 (4.0)	2.98 (3.0)	1267.5	Not Sig $p = .060$
6	I am aware that a password manager will synchronize my passwords across my devices using the vendor's services.	4.0 (4.0)	3.80 (4.0)	1378.0	Not Sig $p = .215$
7	I trust a password manager to delete my password permanently from its database after I delete it from my vault/browser.	3.29 (3.0)	3.18 (3.0)	1526.0	Not Sig $p = .743$
8	I fear that a password manager will fail to work or retrieve my passwords, so I store my passwords in a secondary place.	2.52 (2.0)	2.75 (3.0)	1381.5	Not Sig $p = .231$
9	I fear that all my passwords in a password manager will be exposed if my master password is compromised/stolen.	3.72 (4.0)	3.90 (4.0)	1378.0	Not Sig $p = .463$
10	I write my master password down and store it in a safe place.	2.19 (2.0)	2.37 (2.0)	1310.5	Not Sig $p = .381$
11	I have opened my password manager account on a shared computer.	2.03 (2.0)	2.24 (2.0)	1386.0	Not Sig $p = .236$
12	I would let password manager store my bank details and passport information.	2.82 (3.0)	2.82 (3.0)	1518.0	Not Sig $p = .942$

* Please note that in the published paper [126], the mean (average) numbers are different by one because the range used in the paper is from 0 to 4, while the range used in this table is from 1 to 5.

A few user participants made some interesting comments, for example: “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”, while another wrote “I do not trust password managers, and thus I won’t store the most important passwords in password management services”. So, we can see that user participants do not trust it or don’t know how secure it is. More comments are that: “I only use password manager for unimportant accounts such as shopping websites” and “I store my passwords in it because it is easy to login my accounts”.

5.4 Discussion

In this study, I found interesting findings regarding non-users of password managers. Trust reasons were the most chosen by non-users for not using password managers as they do not trust the vendor to store passwords and do not trust the browser extension to fill in 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 a database because of an attack.

Interestingly, I 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 and non-expert non-users in terms of their perception of password managers, I 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.

In this study, I found that the most used password manager is the built-in manager which is browser-based “Chrome”, which may be related to the ease of access to browsers. Also, I found that more than half of users do not store all passwords in password man-

agers, while half of users do not use random password generator at all. The reasons for not using random password generator are that users do not know how to use it as well as they do not know that password managers offer a built-in random generator. I found that 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 and non-expert users in terms of their perception of password managers, I found no significant difference between them when using password managers which implies that having an education related to computer science or information security does not play any significant factor when using password managers. Also, having an education related to computer science or information security does not play any factor in adopting password managers and does not play any factor to mitigate password reuse.

In regard to the usability of password managers, I found that the users in this study found password managers easy to use, and 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, I found that many users of password managers have security concerns about using a shared computer, they worry about losing stored passwords and the fear of having their passwords exposed if the master password is 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. These findings answer the question on whether users have trust issues and security concerns towards password managers.

5.5 Conclusion

In summary, I found that trust is the problem that makes non-users abstain from using password managers, followed by lack of transparency and security concern while usability is only a minor issue. I also found that many users of password managers have trust and transparency issues towards password managers along with security concern, but they found password managers easy to use. Therefore, there is a need to find a solution that bridges the trust gap between people (users and non-users) and password managers.

So, improving transparency in password managers can be a promising solution to increase the adoption rate of password managers among non-users. It can enhance trust in password managers and lead to a better understanding of the system. I 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 which can help to motivate them to start using password managers and enhance their trust, because when something is visible, people will realize how trustworthy it is. Thus, the impact of improving transparency in password managers will be investigated in the next chapter.

Chapter 6

A User Study about Improving Transparency in Password Managers

6.1 Introduction

In the previous studies (chapter 3, 4 and 5), there were many findings in terms of usability, trust, transparency and security. In regard to the user interface and usability of password managers (chapter 3), I found that cloud password managers mostly satisfied Nielsen's 10 principles, they have good design and offer useful features, but there is a need to improve specific aspects. In the study about usability and trust of password managers (chapter 4), I found that both users and non-users of password managers have trust and transparency issues towards password managers, for example they do not trust password managers to store all passwords, and many of them do not understand how passwords are processed. However, most participants found it easy to create an account, store and access passwords in a password manager.

In the study about users and non-users of password managers (chapter 5), I found that trust is a major problem that makes non-users avoid using password managers, followed by lack of transparency and security concerns, while usability is only a minor issue. I also found that users of password managers have trust and transparency issues towards password managers along with security concerns, but they found password managers easy to use and easy to store passwords. So, based on the results of the three studies (chapter

3, 4 and 5), we can see that current password managers are usable to some extent, while usability is only a minor issue for non-users of password managers. Regarding the aspects of trust, transparency and security, we can see that trust is the main problem that makes non-users avoid using password managers, as well as users have trust issues towards password managers. In addition, users and non-users have transparency issues and security concerns towards password managers.

Therefore, there is a need to bridge the trust gap between people and password managers and improving transparency can be a solution. Because when something is visible, people will realize how trustworthy it is and can increase their confidence in the system, and know that the system will manage their passwords safely. So, improving transparency in password managers can increase the adoption rate of password managers among non-users, as it can enhance trust and lead to a better understanding of the system. As a result, I conduct a study on the impact of improving transparency in password managers and I test the following hypotheses: (1) Improving transparency in password managers leads to a better understanding of the system, and (2) improving transparency enhances trust in password managers.

The results of this study show that the majority of participants know where passwords are stored in a transparent manager compared to a non-transparent manager. Most participants understand how passwords are processed in a transparent manager and how it works compared to a non-transparent one. Likewise, more participants trust a transparent manager to store all their passwords, delete them permanently, store passwords securely and not synchronize them. Also, the vast majority of non-users would like to adopt a password manager if it was the same as a transparent manager. Moreover, there were significant differences between non-transparent and transparent managers in all questions.

6.1.1 The Role of Transparency

The role of transparency was examined in other areas outside password managers. In a study by Sinha and Swearingen about the role of transparency in recommender systems, they stated that users feel confident and like transparent recommendations compared to non-transparent one [130]. In another study on using a transparency tool to display users' data that were collected and stored at the services' side, Angulo *et al.* stated that security and privacy features have to be made clear to users so that they can trust the transparency tool [131]. Moreover, Sugatan and Schaub used interactive stories for security education, they found that participants were confident that password managers would keep their passwords safe and protect them [132].

Similarly, to investigate the effects of transparency on users' experience and privacy, Vitale *et al.* compared between non-transparent and transparent user interfaces in robot systems. The transparent conditions have additional stages than non-transparent conditions such as informing the user about algorithm used in the face recognition, how data is recorded and stored and legal privacy policies. They found that a transparent system leads to a more positive experience for users compared to a non-transparent one and has positive effects on perceived attractiveness and stimulation [133]. In a study of transparency, Herlocker *et al.* found that making a process transparent will increase users' willingness to use the system and build their confidence in it [134].

So, we can see that educating people, improving transparency and allowing interaction can enhance trust in the system, increase confidence and willingness to use such a system. As a result, I conduct this study in order to test the following hypotheses: (1) Improving transparency in password managers leads to a better understanding of the system, and (2) improving transparency enhances trust in password managers.

6.2 Design a Prototype of Password Managers

I designed a prototype for this study using ASP.NET Core (C#). The prototype is a website that can be accessible from all popular web browsers on different devices such as Chrome, Firefox and Safari. I used the default design, while the user interface of the systems will change based on the screen size of the device. I can also reach a higher number of participants who use laptops/desktops, smartphones and tablets; therefore, this variety of devices can enrich the study. For more screenshots of the user interface of the two programs, please see the appendix section ([A.6](#)).

To take part in the study, participants should read the information and instructions about the study on the home page (Fig 6.1). In detail, a non-transparent password manager (PM) is similar to current password managers where the user only stores a password but does not know or see how things work in the system. On the other hand, a transparent password manager (PM) offers more insights into how a password manager works. Participants can interact in specific steps such as generating an encryption key, choose a place to store their password and allow password synchronization. A validation messages are used to alert participants in case they forget to insert mandatory details such as a password.

Participants were asked to start the study using a non-transparent PM, where they add an account and save it (Fig 6.6), update their password and view details of their account (Fig 6.4). After that, they use a transparent PM by adding an account (Fig 6.6), then update it and finally view the details of their account (Fig 6.4). In the transparent PM, participants can generate an encryption key and know its algorithm (e.g., AES) and length; thus, it will boost their understanding and trust. Participants can only generate an encryption key at a high level (click on a button), because it might be complicated for them if they interact via many steps to generate a key.

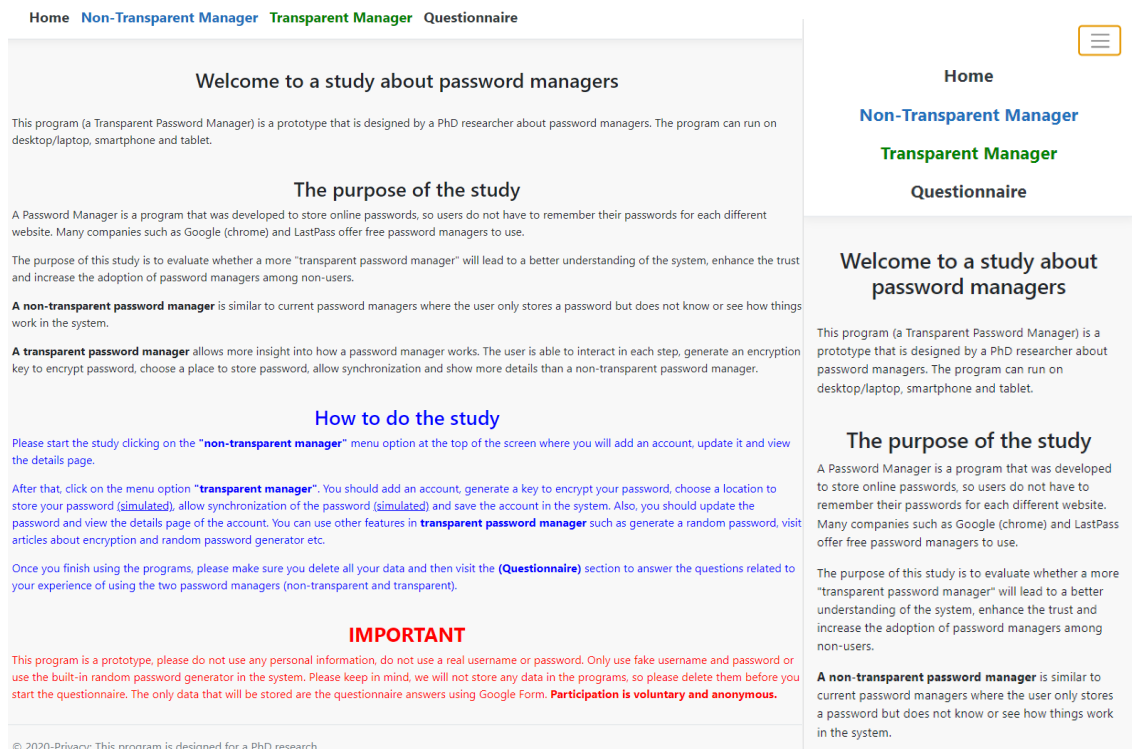


Figure 6.1: Homepage of the website (prototype) which shows information and instructions about the study. A screenshot from a desktop (left) and a smartphone (right).

Non-Transparent Home Page			
Add a new account			
Username	Password	Website Name	Website URL
Example	abc123	Twitter	Twitter.com
Update Details Delete			

Figure 6.2: Main page of a non-transparent PM. It shows a stored account, website name/URL, username and plain password.

Transparent Home Page				
Add a new account				How system works ?
Username	Password (Encrypted)	Website Name	Website URL	Time of storing
Example	cC0w7dZ6ji6fzl2J wvSdlQ==	twitter	www.twitter.com	2020-06-24 15:33:21
				Update Details Delete

Figure 6.3: Main page of a transparent PM. It shows a stored account, website name/URL, username, encrypted password and time of storing it. Also, there is an image embedded on the top right explaining how the system works.

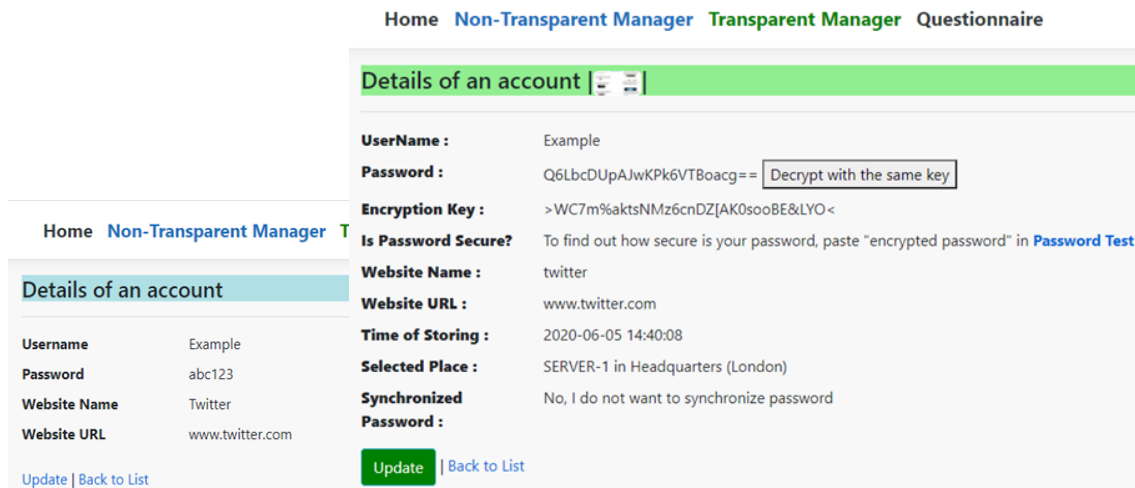


Figure 6.4: Details of a non-transparent manager page (left), it only shows a username, plain password and website name/URL. Details page of a transparent manager (right), as participants can see an encrypted password, encryption key, time of storing, location and synchronization. The password can be decrypted using the same key and an image is embedded at the top which is about how the system works. Also, there is an external link to check the strength of password provided on the details page.

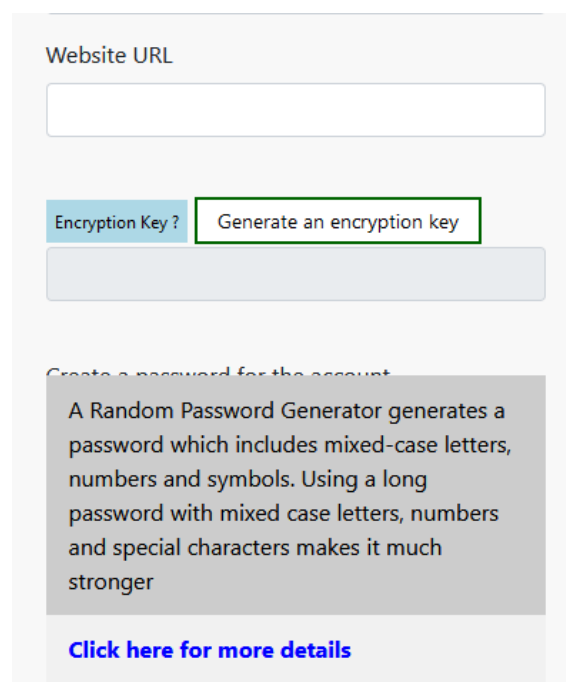


Figure 6.5: The text box is about a random password generator and an advice of using one. Also, a website link is embedded which explains about password generator.

The figure shows two side-by-side screenshots of 'Add a new account' forms. The left screenshot (non-transparent PM) features a light blue header, input fields for Username, Website Name, and Website URL, a password field with a strength indicator (red, yellow, green bars), and a 'Save' button. The right screenshot (transparent PM) has a light green header and includes an 'Encryption Key?' section with a 'Generate an encryption key' button. It also features a password generator with a 'Why Generator?' link and strength indicators (Very Weak, Weak, Average, Strong, Very Strong). Below the password field, it shows a map selection interface with options like 'Map of Headquarter', 'Map of 2nd branch', and 'Map of Google company', a dropdown for 'What is this?' (SERVER-1 in Headquarters (London)), and a synchronization question: 'Do you want to synchronize your password over different devices...?' with a 'Yes, I want to synchronize password' option. Both forms include an 'Encrypt & Save' button and a 'Back to List' link. A footer note reads: '© 2020-Privacy: This program is designed for a PhD research'.

Figure 6.6: Adding an account in a non-transparent PM (left), there are only forms for username, password and website name/URL. Password generator buttons are in colour. Adding an account page in a transparent PM (Right), participants can generate an encryption key, know its length and the algorithm used. They can choose a place to store each password and view the location on Google maps (simulated). They can generate a random password using a generator which shows the strength of password in words and colours. They can allow or prevent password synchronization for each password (simulated).

In the transparent PM (Fig 6.6), participants can choose a place to store their password (only simulated), and view the location on Google maps; hence, it will increase their understanding and trust in the system to store passwords and let them feel that they have control of their passwords. Likewise, participants can either accept or reject having their passwords synchronized with other devices (only simulated). The idea of asking participants about synchronization is to assure them that the transparent manager will not synchronize passwords without their permission, so it can enhance their trust and let them know that they are in control of their passwords. The transparent PM (Fig 6.4) shows participants the encrypted password and encryption key and allows them to decrypt their

password and shows them the date and time of storing it. Please note that none of these steps and features are available in the non-transparent manager.

Participants can use a random password generator to generate a unique password when using non-transparent and transparent managers, so they can understand the benefit of having a unique password for each account. In the transparent manager (Fig 6.5), a text box and a website link are embedded into the page with the purpose of educating participants about the benefits of random password generators.

Finally, I informed the participants that the program is a prototype (Fig 6.1), so they should not use any personal information, real usernames or passwords in this study. They should only use fake usernames and passwords, or they can use the built-in random password generator. Participation is voluntary and anonymous.

6.3 Methodology

The purpose of this study is to evaluate whether improving transparency in password managers will lead to a better understanding of and enhance trust in the system. I tested the hypotheses through participants' answers when using non-transparent and transparent password managers.

I used an online questionnaire to reach out to more participants, with a broader age range and different education levels and participants who use different devices and operating systems. I designed the questionnaire using Google forms, which is a free service, and embedded a link (URL) to the questionnaire into the website (prototype). To recruit participants, I distributed the link to the study (prototype) online via social media platforms such as LinkedIn and WhatsApp; also, I distributed the link across Cardiff university by email. After collecting the data, three repeated answers and ten inconsistent answers were discarded. Thus, the overall number of valid responses is 132.

The online questionnaire contains two parts, the first part is for general questions

while the second part has two sections: a section for non-transparent PM and another for transparent PM. Eleven identical questions (ranging from strongly disagree “1” to strongly agree “5”) are about understanding and trusting non-transparent and transparent password managers, also whether passwords are stored securely. There are five questions to test the first hypothesis “lead to a better understanding of the system” and four questions for the second hypothesis “enhance trust in password managers”. Another question is for non-users of password managers which is about the adoption of a transparent manager.

Please note that closed-ended questions (multiple choice, multiple options, Likert scale) were analyzed quantitatively and SPSS program was used for statistics, while open-ended questions were analyzed qualitatively. I used more questions to understand participants’ views regarding the usability of transparent manager, such as the things they like and dislike, and the System Usability Scale (SUS) questions [124], [125] (For all questions). This study was reviewed and approved by the School of Computer Science Research Ethics Group, Cardiff University, UK.

6.4 Result

There are 132 participants who completed the study; 25% are aged 18–25 years, 39% are aged 26–35, and 25% are between 36–45, while only four participants are aged 56–65. So, 64% of the participants are less than 35 years old and there are more males than females (72% vs. 27%). Regarding the education level of the 132 participants, 39% have a bachelor’s degree, 34% a master’s degree and 13% are PhD holders. From these results, we can see that the majority of participants (86%) are well educated.

Regarding the educational background of participants, as mentioned in the previous chapter (chapter 5), I considered participants with an educational background related to computer science or information security as experts. Fifty-six participants (42%) have an educational background related to computer science or information security, while 76 participants (58%) have one that is not related to computer science or information security.

So, there are 58% non-experts and 42% experts in this study (table 6.2).

I also found that 8% of the participants have 1 to 5 accounts, 29% have 6 to 10 online accounts and 22% have 11 to 15 accounts. Also, 11% participants have 16 to 20 accounts and 29% have 21 accounts or more. With regard to the number of online passwords, 62% of participants have 1 to 5 passwords, 21% have 6 to 10 passwords, 3% participants have 11 to 15 passwords and 11% have 21 passwords or more.

Table 6.1: Number of online passwords for 132 participants.

Passwords	Participants
1 to 5	62%
6 to 10	21%
11 to 15	3%
16 to 20	0%
21 or more	11%
I do not know	3%

Table 6.2: Number of experts and non-experts.

Experts	Non-Experts
56 (42%)	76 (58%)

In this study, I designed a prototype which works on different devices (multi-platforms). I found that 57 participants (43%) used a laptop/desktop when they did the study, seventy-four participants (56%) used a smartphone, while only one participant used a tablet (table 6.3). I also found that 70 participants (53%) are users of password managers while 62 participants (47%) are non-users of password managers. For the 70 users of password managers, the most used password manager is Chrome followed by LastPass and others use Firefox and Dashlane.

Table 6.3: Type of devices used in this study

Laptop/Desktop	Smartphone	Tablet
57 (43%)	74 (56%)	(1) 1%

Table 6.4: Number of users and non-users of password managers.

Users	Non-Users
70 (53%)	62 (47%)

6.4.1 Comparing Non-transparent and Transparent Managers

As stated earlier, the hypotheses is that improving transparency in password managers leads to a better understanding of the system, and enhances trust in password managers. One hundred and thirty-two participants answered 11 questions about a non-transparent PM and another 11 identical questions about a transparent PM (ranging from strongly disagree “1” to strongly agree “5”).

I found that there are only 27% of participants who know the location of a stored password in a non-transparent PM compared to 77% who know the location of a stored password in a transparent PM. So, the majority of participants know the location when they use the transparent PM. The reason for seeking this answer is that participants can choose the location to store an account/password in a transparent manager and they can even see the location on Google maps (simulated).

Table 6.5: I know where my online passwords are stored.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	7%	20%	21%	35%	17%
Transparent	33%	44%	10%	11%	2%

In regard to the process in non-transparent and transparent managers, 23% of participants understand the process of storing passwords in a non-transparent PM compared to 69% who understand the process in a transparent manager. From these findings, we can see that most participants understand how passwords are processed when they use a transparent PM. The reason for eliciting this result is that participants can generate an encryption key and encrypt a password, they know the algorithm used and decrypt a pass-

word in the transparent PM.

Table 6.6: I fully understand how my passwords are processed.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	7%	16%	16%	46%	15%
Transparent	12%	57%	16%	12%	3%

I also found that 32% of participants understand how a non-transparent manager works compared to 69% who understand how a transparent manager works. So, most participants understand the way a transparent PM works and the reason can be related to the fact that they can use transparent PM with functions that allow them to understand how it works internally, such as generating an encryption key, choosing the place to store a password, allowing or rejecting synchronization and saving an encrypted password. Also, they can view an image that shows how transparent PM works.

Table 6.7: I understand how it works.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	8%	24%	28%	32%	8%
Transparent	14%	55%	18%	10%	3%

Moreover, only 22% understand the way a non-transparent manager generates an encryption key while 54% of participants understand it in a transparent manager. The reason for having this result is that the participants only needed to press a button to generate an encryption key when using the transparent manager and could see the key on the screen. Thus, they understand where the key comes from, while they do not see anything in non-transparent manager. For this question, participants were only able to generate an encryption key in the transparent manager in a very simple way.

Table 6.8: I understand how it generates the encryption key.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	5%	17%	20%	44%	14%
Transparent	17%	37%	29%	14%	3%

Regarding understanding the benefits of a random password generator in non-transparent and transparent managers, I found that 58% understand the benefits in the non-transparent manager, while 73% understand the benefits in the transparent manager. A possible explanation of these answers is that I only used colours for generating passwords buttons in the non-transparent manager, while I used colours and labels for buttons in the transparent manager along with a text box and a website link (URL) which explains the benefits of a random password generator. These results imply that most participants understand the benefits of a password generator with colours as well as labels. The colours used for the buttons are suitable for the strength of passwords.

Table 6.9: I understand the benefit of a random password generator.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	16%	42%	21%	17%	4%
Transparent	29%	44%	15%	10%	2%

In addition, 36% of participants trust a non-transparent manager to store all passwords compared to 65% who trust a transparent manager. From this finding, we can see that more than half of participants trust a transparent PM to store all their passwords. The reasons may be related to them encrypting their password themselves, choosing the location to store it which can be on their own device, and seeing the encrypted password on the main page which increases their trust in a transparent manager. Meanwhile they do not see any encryption, location or process in a non-transparent one.

Table 6.10: I trust it to store all my online passwords.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	7%	29%	28%	25%	11%
Transparent	18%	47%	26%	8%	1%

Also, I found that 27% of participants trust a non-transparent manager to delete passwords permanently compared to 59% who trust a transparent manager. So, more participants trust a transparent manager than a non-transparent manager. The reason may be related to participants being involved in the steps when using a transparent manager such as storing a password in a preferred place which can be on their own device and preventing password synchronization. The transparent manager shows a confirmation message when deleting a password permanently which is not in a non-transparent manager.

Table 6.11: I trust it to delete my password from its database permanently after I have deleted it from my account.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	7%	20%	21%	32%	20%
Transparent	12%	47%	29%	11%	1%

In regard to trusting non-transparent and transparent managers to generate a strong key to encrypt password; 41% of participants trust a non-transparent manager to generate a strong key to encrypt their password compared to 74% who trust a transparent manager. From these results, it appears that the majority of participants trust a transparent manager more than a non-transparent manager. The reason behind this answer is that participants generate the encryption key themselves, they know the algorithm and its length, and they can see the encrypted password and key together. Meanwhile, all these steps and features do not exist in a non-transparent PM.

Table 6.12: I trust it to generate a strong key to encrypt my password.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	11%	30%	26%	26%	7%
Transparent	22%	52%	25%	1%	0%

Furthermore, 30% of participants feel they have control of passwords when storing them in a non-transparent manager compared to 70% for a transparent manager. The reason behind this result may be because participants choose the location to store passwords which can be on their own device or on Google drive, so they know that they are in control of the passwords. They can see more details about stored passwords in a transparent manager which are not visible in a non-transparent manager. Plus, they can prevent password synchronization to other devices (simulated). So, this result shows that allowing participants to be involved in a few steps while using the program can make them feel they are in control of their own passwords.

Table 6.13: I feel that I have control of my passwords when I store them.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	7%	23%	33%	23%	14%
Transparent	16%	54%	21%	8%	1%

Regarding storing passwords securely in non-transparent and transparent managers, I found that 33% believe that a password is stored securely in a non-transparent manager compared to 67% who believe a password is stored securely in a transparent manager. Interestingly, 47% of participants are neutral about a non-transparent PM which can mean that they lean towards thinking the system might not be secure. However, most participants believe that a password is stored securely in a transparent PM which implies that allowing participants to store passwords in a preferred location, and showing them the encrypted password, will reassure them about the strong security of the system.

Table 6.14: Password is stored securely in it.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	7%	26%	47%	16%	4%
Transparent	12%	55%	30%	2%	1%

As is known, some password managers synchronize all passwords to users' devices, while users might prefer not to synchronize all their passwords. In this study, only 28% of participants trust a non-transparent manager for not synchronizing passwords over different devices without permission compared to 67% who trust a transparent manager. So, the results prove that allowing participants to decide about synchronizing each password at the stage of adding it to the system can increase their trust, also participants can see that a password is only stored in their chosen place along with the date and time, which does not occur in a non-transparent manager.

Table 6.15: I trust it for not synchronizing my passwords over different devices (e.g., computers, smartphones) without my permission.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Non-transparent	8%	20%	36%	26%	10%
Transparent	19%	48%	26%	5%	2%

So, based on the findings from the 11 questions about both password managers, we can see that improving transparency leads to a better understanding of the system as well as enhancing the trust in password managers.

In addition, to determine if there are any significant differences between non-transparent and transparent password managers via the 11 questions that were answered by the 132 participants, I used a Wilcoxon Signed-Ranks test, because it compares two scores that come from the same participants (Table 6.16), while the p-value of .000 is reported as .001 as recommended by [127], [128]. I found that there were significant differences between non-transparent and transparent managers in answer to all 11 questions, so the findings statistically confirm the hypotheses: improving transparency in password managers leads

to a better understanding of the system, and enhances trust in password managers.

For example, a Wilcoxon signed-rank test shows that a transparent manager (median = 4.0) is trusted to delete passwords permanently more than a non-transparent manager (median = 2.0) and the difference is significant ($Z = -6.781$, $p < .001$). Likewise, a Wilcoxon signed-rank test indicates that participants know where passwords are stored in the transparent manager (median = 4.0) more than the non-transparent manager (median = 2.0) and the difference is significant, ($Z = -7.197$, $p < .001$).

Table 6.16: Comparing between non-transparent (Non) and transparent (Tra) password managers using a Wilcoxon Signed-Ranks test. The table shows the mean (average) and median, Z score and p-value of each statement.

	Statements	Mean & (Med.) of Non	Mean & (Med.) of Tra	Z score	p-value .05
1	I know where my online passwords are stored.	2.64 (2.0)	3.93 (4.0)	-7.197	Sig $p < .001$
2	I fully understand how my passwords are processed.	2.53 (2.0)	3.63 (4.0)	-7.268	Sig $p < .001$
3	I understand how it works.	2.94 (3.0)	3.67 (4.0)	-5.842	Sig $p < .001$
4	I understand how it generates the encryption key.	2.56 (2.0)	3.50 (4.0)	-6.918	Sig $p < .001$
5	I understand the benefit of a random password generator.	3.48 (4.0)	3.87 (4.0)	-3.575	Sig $p < .001$
6	I trust it to store all my online passwords.	2.95 (3.0)	3.74 (4.0)	-5.497	Sig $p < .001$
7	I trust it to delete my password from its database permanently after I have deleted it from my account.	2.61 (2.0)	3.58 (4.0)	-6.781	Sig $p < .001$
8	I trust it to generate a strong key to encrypt my password.	3.12 (3.0)	3.94 (4.0)	-5.982	Sig $p < .001$
9	I feel that I have control of my passwords when I store them.	2.86 (3.0)	3.77 (4.0)	-5.917	Sig $p < .001$
10	Password is stored securely.	3.17 (3.0)	3.75 (4.0)	-5.241	Sig $p < .001$
11	I trust it for not synchronizing my passwords over different devices without my permission.	2.90 (3.0)	3.78 (4.0)	-5.984	Sig $p < .001$

Non-users of Password Managers:

Of 132 participants, 62 participants do not use password managers. I asked them if they would be willing to adopt a transparent password manager; the answer is that 50 (81%) non-users answered “Yes”, while 12 non-users answered “No”. I asked the 50 non-users who answered “Yes”; why they would be willing to use a transparent password manager and I gave them four potential reasons as options to choose from. The reasons most selected are as follows: 30 non-users chose “I understand how it works”, 26 chose “it is trustworthy”, 20 chose “it is secure” and 18 chose “it is easy to use”.

On the other hand, for the 12 non-user participants who answered “No”, some of them stated their reasons which are related to a trust issue and security concerns. For example, participants stated that they do not trust a password manager, and passwords will be available to a hacker if the device is hacked. Other participants reported similar trust and security concerns about using the manager such as they do not feel safe, they never trust any program to handle passwords and they would not feel comfortable. One non-user gave a different reason which is “what you call a transparent password manager just contains some more information and details of the process. I can only trust it if I have the sources and compile it myself. Anything else can still just be pretending”.

6.4.2 Usability of Transparent Password Manager

In the last section of the questionnaire, the 132 participants answered a set of questions about the language used, the design, the most liked and disliked, and System Usability Scale (SUS) [135] of the transparent manager (Fig 6.7). The purpose of asking these questions is to understand how usable and suitable a transparent manager is, plus I can compare between laptop and smartphone users, experts and non-experts, and users and non-users using SUS scores.

Regarding the language used in a transparent manager, I found that 24% are very sat-

ified, 56% are satisfied with the language used, 18% of participants are neither satisfied nor dissatisfied, while only two participants are dissatisfied. So, using less computer jargon and very simple language makes it easy to read and understand the information. As for the design and layout of a transparent PM, I found that only 14% of participants found it excellent, 52% found it good, while 28% found it average. Also, five participants found the design fair and only two participants found it poor.

The 132 participants answered ten questions on a System Usability Scale (SUS). The System Usability Scale covers different aspects such as support and complexity [125]. I found that the SUS score for all types (desktop/laptop, smartphone and tablet) is 65.02. From figure 6.7, we can see that a transparent manager is a marginal high acceptable program which is closer to the rate “Good”. All participants’ answers to SUS questions can be found in table 6.18.

Table 6.17: System Usability Scale (SUS) Score.

Type of participants	Average SUS score
All 132 participants	65.02
56 Experts 76 Non-experts	67.14 63.45
70 Users 62 Non-users	65.39 64.60
57 Laptop/desktop users 74 Smartphone users	66.84 63.55

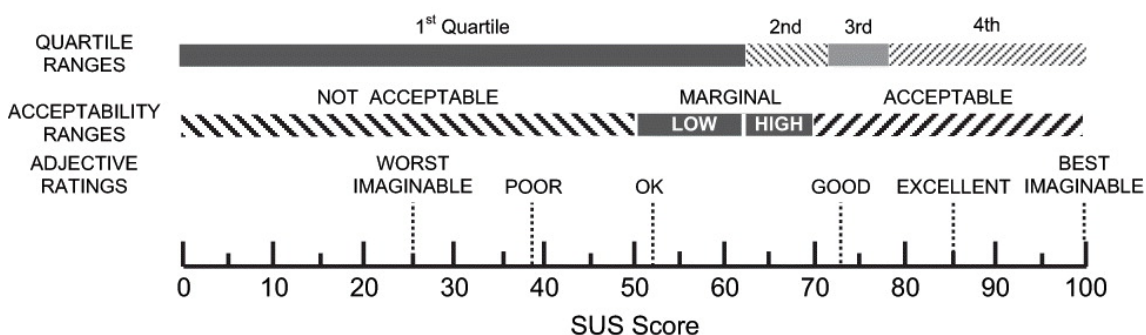


Figure 6.7: System Usability Scale (SUS) scores. The figure is taken from an article for Bangor *et al.* [135], An empirical evaluation of the system usability scale.

I also found that the SUS score for experts is 67.14 while the SUS score for non-experts is 63.45. So, I can see that experts found a transparent manager more usable compared to non-experts because non-experts might need help from a technical person to use a transparent manager while experts are more familiar with programs. In regard to users and non-users of password managers, the SUS score for users is 65.39 while the score is 64.60 for non-users. Both scores are very similar between the two groups. For participants who use a desktop/ laptop or a smartphone, the SUS score for desktop/laptop is 66.84 while it is 63.55 for smartphone users. These scores mean that desktop/laptop users found a transparent PM more usable compared to smartphone users.

Table 6.18: SUS questions were answered by 132 participants about transparent manager.

	Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	I think that I would like to use this system frequently.	18%	61%	15%	5%	1%
2	I found the system unnecessarily complex.	3%	15%	28%	47%	7%
3	I thought the system was easy to use.	17%	59%	17%	5%	2%
4	I think that I would need the support of a technical person to be able to use this system.	4%	23%	17%	36%	20%
5	I found the various functions in this system were well integrated.	10%	58%	30%	0%	2%
6	I thought there was too much inconsistency in this system.	3%	9%	27%	49%	12%
7	I would imagine that most people would learn to use this system very quickly.	14%	55%	23%	6%	2%
8	I found the system very cumbersome to use.	5%	13%	33%	39%	10%
9	I felt very confident using the system.	14%	58%	23%	5%	0%
10	I needed to learn a lot of things before I could get going with this system.	10%	18%	30%	27%	15%

Furthermore, I asked the participants two open-ended questions about the things they

like and dislike about a transparent PM. The comments from the two questions were analyzed qualitatively using inductive coding. The things participants liked the most about a transparent PM are that it is trustworthy, informative, a transparent tool and the ability to manage passwords (table 6.19). So, the comments show that the transparent manager increases trust among participants and educates them as well.

Table 6.19: Comments sample about the things they like most in a transparent manager.

Code	Sample of comments
Manage passwords	<ul style="list-style-type: none"> • The consideration about where the data is stored, offering local storage instead • The ability to choose more. I felt it would be useful for me, providing good ToS, etc • The ability to decide where the password is stored. It had never occurred to me to consider where my passwords are actually stored. • Makes you feel controlled over your passwords. • Gives the user more control over their personal data.
Trustworthy	<ul style="list-style-type: none"> • Boosting user confidence in the password manager, for example i simply thought that my passwords were saved without encryption. but seeing the transparent password manager in action greatly increased my trust in password managers and improved my understanding. • I trust transparent more, I know where my account is stored. more information about password generator.
Transparent tool	<ul style="list-style-type: none"> • Reassuring to show where physical location of where passwords are saved. • I can see the encryption key used for my passwords and where they are stored. • Whilst it's a good idea to use encryption key however I would like to have seen different types of encryption keys.
Informative	<ul style="list-style-type: none"> • The tooltips explaining the different components and how they work. • Easy to understand when explained.

In contrast, the things that participants disliked the most in a transparent PM are that the user interface is not flexible, it is not user friendly and there is a security concern about stored passwords and encryption keys (Table 6.20).

Table 6.20: Comments sample about the things they dislike most in a transparent manager.

Code	Sample of comments
User interface not flexible	<ul style="list-style-type: none"> • On smartphone the box sizes in the table do not scale so smaller responses still have larger boxes making it harder to use. • A better GUI would be more attractive to the user.
Not user friendly	<ul style="list-style-type: none"> • It is very clearly a proof-of-concept prototype, and there's nothing wrong with that. I think it would need a lot of IxD work for it to be functional for novice users, though. For one thing, the explanations need work (but again, PoC. It's good that they're there), and I would have liked to be able to set up a "standard settings" profile or similar if I were to use it as my regular password manager. I don't want to have to choose where to store my passwords every time, as I would like to have them all in one (specific) place. • It takes longer to set one up. • It might require technical help for people who are not familiar with technology and words like encryption and server location might confuse them and therefore they will not be confident in using the system.
Security concern	<ul style="list-style-type: none"> • I feel like allowing people to choose their own encryption key is dangerous, especially if you are trying to encourage use among less computer-savvy people. • I have only one concern, with location of the where my passwords are stored is exposed I.e. London/cardiff branch what if with this information hackers can make this a target to collect my login information such as my online banking details.

Finally, some participants made comments regarding this study. One participant said that it is a very enlightening study that made them aware of matters that never occurred to them before such as password storage location. Also, other participants suggested a few things to improve the transparent manager, for example, a participant said "I feel I would not have much trouble understanding and using the system but a non technical user might have more problems". One participant stated that "if possible to open many choices in the area of encryption, this would raise the confidentiality of work and designing a good product".

6.5 Discussion

Previous studies on password managers focused mostly on improving security and usability, and to the best of my knowledge, there have been no studies about improving transparency in password managers. The finding of this study is that participants found a transparent manager understandable and trustworthy compared to a non-transparent manager. I found that there were significant differences between non-transparent and transparent managers which answered the hypotheses: (1) improving transparency leads to a better understanding of the system, and (2) enhances trust in password managers. Also, I found that the majority of non-users are more willing to adopt a tool if it was like a transparent manager.

In this study, I found that the majority of participants know where passwords are stored in a transparent manager compared to a non-transparent manager. Most participants understand how passwords are processed in a transparent manager and how it works compared to a non-transparent manager. Importantly, more participants trust a transparent manager to store all their passwords, delete them permanently, store passwords securely and not synchronize them without permission. So, allowing people to generate an encryption key, choose a location to store a password and be involved in many steps can be strong ways to solve the trust issue in password managers because a lack of trust was a reason for non-users not to use a password manager.

Additionally, by allowing people to encrypt and decrypt a password and show an encrypted password on a screen can overcome security concerns with password managers. Please note that allowing users, particularly non-technical, to choose a key themselves can be a security problem because they might choose a weak encryption key, thus, they must only use strong encryption keys. In regard to the storage location, it should be shown only to users and no one else can know about it. Moreover, providing more details and allowing people to be involved in each step, such as generating an encryption key, will increase their awareness and understanding of how the system works.

In the study, most participants understand the benefits of a random password generator in a non-transparent manager even though the strength of passwords (buttons) is only represented by a few colours. This implies that they know the benefits of a password generator. Hence, I believe that a password generator should have visible buttons placed around a password form in order to make it easy to reach them and encourage people to use them.

The overall SUS score for a transparent manager is 65.02, which is a marginal high acceptable. The most liked things in the transparent PM are that it is informative and trustworthy (table 6.19), while the most disliked things are that the user interface is not flexible and there is a security concern about stored passwords (table 6.20). So, the idea of improving transparency in password managers is enlightening and raised awareness of password storage as well as enhancing trust.

6.6 Conclusion

To conclude, the finding of this study is that improving transparency leads to a better understanding of the system and enhances trust in password managers. For example, most participants knew where passwords are stored in a transparent manager as well as they trust the transparent manager to store all passwords. Also, there were significant differences between transparent and non-transparent managers in 11 questions. Regarding non-users of password managers, the majority of them would adopt a transparent manager.

In the next chapter, I repeated the same study as the study in this chapter but with some changes in order to ensure that participants will not be influenced by words or biased language. Thus, I can discover if making the changes in the extended study will affect the outcome of this study.

Chapter 7

An Extended User Study about Improving Transparency in Password Managers

7.1 Introduction

In this chapter, I do the same study as the previous chapter with some changes to ensure that participants will not be driven by words or biased language. I want to find out if making these changes will affect the outcome of the previous study or it will prove and confirm it. More specifically, the changes I made are as follows:

- The name of the non-transparent password manager was called “Program A” while the transparent manager was called “Program B”.
- The introduction page of the website was amended to remove any details about both programs to make sure that it will not influence participants towards any program.
- Participants were asked to start using program A and B or vice versa, I added a question about it in the questionnaire to find out which program was used at first to ensure randomization.
- Asterisks were added in program A to hide the password, so it can be similar to current password managers such as Chrome.

- A question was added for all participants about which program they prefer (A or B) and a set of questions were added to find out the reasons why they preferred it.

The results of this study prove and confirm the results of the previous study (non-transparent and transparent managers). The results show that the majority of participants know the place of passwords and they understand the process in program B compared to program A. Most participants understand how program B works compared to program A. Also, more participants trust program B to store all their passwords, delete them permanently and store passwords securely. I found that 75% of participants preferred program B, and that the provided features are important to them. Importantly, there were significant differences between program A and B which answers and confirms the hypotheses.

7.2 Design a Prototype of Password Managers

For the extended user study, the names of the programs were changed to be program A and program B (Figure 7.1). There is also a slight change to program A for the stored password (Figure 7.2) as I used asterisks to hide the password to imitate current password managers such as Chrome. The rest remains the same as in the previous chapter for both programs.

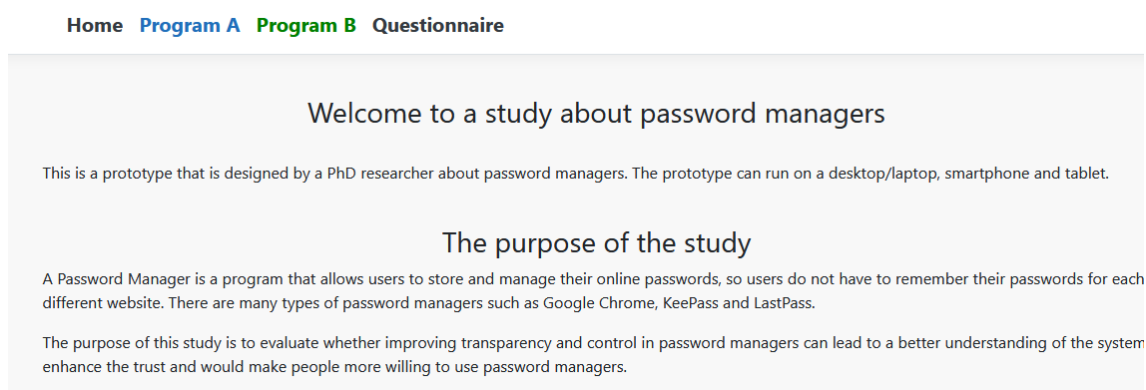


Figure 7.1: Homepage of the website which shows information and instructions.

Username	Password	Website Name	Website URL
Example	***** 321	Twitter	Twitter.com

Figure 7.2: Main page of program A. It shows a website name/URL, username and a password as asterisks (it only shows the password when a user puts the cursor on the eye icon).

7.3 Methodology

I used the same methodology for this study as in the previous study. I only amended the questions to refer to program A and program B rather than non-transparent and transparent. Also, a new set of questions was added to find out which program is preferred by participants, and which factor in program B is important for participants (range from not important at all to very important). Please note that I added two questions that are not related to the programs in order to find the invalid answer. For example, Madrid is the capital of France, so I can find out if participants paid attention while answering the questionnaire (For all questions). After collecting the data, two repeated answers and four inconsistent answers were discarded. Thus, the overall number of valid responses is 68. This study was reviewed by Computer Science and Informatics Ethics Committee and received a favourable opinion, Cardiff University, UK.

7.4 Result

There are 68 participants who completed the study; 22% are aged 18–25 years, 60% are aged 26–35, and 12% are between 36–45, while only 2 participants are aged 46–55. So, 82% of the participants are less than 35 years old and there are more males than females (81% vs. 19%). Regarding the education level of the 68 participants, 32% have a bachelor's degree, 41% a master's and 18% are PhD holders. From these results, we can see that the majority of participants are well educated.

Regarding the educational background of participants, as mentioned in chapter 5, I considered participants with an educational background related to computer science or information security as experts. Thirty-one participants (46%) have an educational background related to computer science or information security, while 37 participants (54%) have one that is not related to computer science or information security. So, there are 54% non-experts and 46% experts in this study (table 7.1).

In this study, thirty-one participants (46%) used a laptop/desktop when they did the study and thirty-seven participants (54%) used a smartphone (table 7.2). Regarding the number of users and non-users of password managers in this study, I found that 36 participants (53%) are users of password managers while 32 participants (47%) are non-users (table 7.3). I also found that 63 participants (93%) used program A first and then program B, while 5 participants used program B first and then program A.

Table 7.1: Number of experts and non-experts.

Experts	Non-Experts
31 (46%)	37 (54%)

Table 7.2: Type of devices used in this study

Laptop/Desktop	Smartphone
31 (46%)	37 (54%)

Table 7.3: Number of users and non-users of password managers.

Users	Non-Users
36 (53%)	32 (47%)

In regard to the number of accounts, 7% of the participants have 1 to 5 accounts, 27% have 6 to 10 accounts and 28% have 11 to 15 accounts. Also, 28% have 21 accounts or more. With regard to the number of passwords, 63% of participants have 1 to 5 passwords, 19% have 6 to 10 passwords, 9% have 11 to 15 and 6% have 21 passwords or more.

Table 7.4: Number of online passwords for 68 participants.

Passwords	Participants
1 to 5	63%
6 to 10	19%
11 to 15	9%
16 to 20	2%
21 or more	6%
I do not know	1%

7.4.1 Comparing Program A and Program B

Regarding the location of stored passwords, I found that 43% of participants know where passwords are stored in program A compared to 73% who know the location of a stored password in program B. So, the majority of participants know the location when they use program B. The reason for this is that participants can choose the place to store an account/password in program B.

Table 7.5: I know where my online passwords are stored.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	19%	24%	12%	26%	19%
Program B	32%	41%	18%	5%	4%

I found that 50% of participants understand the process in program A compared to 81% who understand the process in program B. So, the majority of participants understand how passwords are processed when using program B. The explanation for this result is that participants can encrypt and decrypt password and know its algorithm in program B.

Table 7.6: I fully understand how my passwords are processed.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	18%	32%	19%	18%	13%
Program B	25%	56%	12%	4%	3%

Moreover, 56% of participants understand how program A works compared to 77%

who understand how program B works. So, most participants understand the way program B works and the reason for this could be related to the way that they interact in different steps with program B, such as generating an encryption key and choosing the location to store a password.

Table 7.7: I understand how it works.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	16%	40%	22%	19%	3%
Program B	25%	52%	13%	7%	3%

Also, 30% understand the way program A generates an encryption key while 76% of participants understand it in program B. The reason for this result is that the participants only needed to press a button to generate an encryption key when using program B and they could see the key on the screen.

Table 7.8: I understand how it generates the encryption key.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	7%	23%	24%	31%	15%
Program B	22%	54%	13%	9%	2%

For the random password generator in program A and B, the result shows that 62% understand the benefits of a random password generator in program A while 83% understand its benefits in program B. These results imply that the majority of participants understand the benefits of a random generator with colours as well as labels.

Table 7.9: I understand the benefit of a random password generator.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	22%	40%	19%	19%	0%
Program B	40%	43%	12%	4%	1%

Furthermore, only 31% of participants trust program A to store all passwords com-

pared to 75% who trust program B. From these findings, we can see that most participants trust program B to store all passwords. The reasons can be related to them encrypting their password themselves, choosing the place to store the password which can be their own device, and seeing the encrypted password on program B which increases trust.

Table 7.10: I trust it to store all my online passwords.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	4%	27%	28%	32%	9%
Program B	26%	49%	21%	1%	3%

I found that 38% of participants trust program A to delete passwords permanently compared to 66% who trust program B. So, most participants trust program B more than A and the reason might be related to participants being involved in the steps when using program B such as storing a password in a preferred place and preventing password synchronization to other devices.

Table 7.11: I trust it to delete my password from its database permanently after I have deleted it from my account.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	10%	28%	30%	22%	10%
Program B	28%	38%	29%	3%	2%

Additionally, 28% of participants trust program A to generate a strong key to encrypt passwords compared to 82% who trust program B. The results show that the majority of participants trust program B more than program A and the reason behind this answer is that participants generate the encryption key, they know the algorithm and its length.

Table 7.12: I trust it to generate a strong key to encrypt my password.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	6%	22%	25%	31%	16%
Program B	37%	45%	15%	3%	0%

I also found that 38% of participants feel they have control of passwords when storing them in program A compared to 70% for program B. The reason might be because participants choose the location to store passwords which can be on their own device. They can see the date and time of the stored passwords in program B which are not visible in program A. Plus, they can prevent password synchronization to other devices.

Table 7.13: I feel that I have control of my passwords when I store them.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	10%	28%	28%	28%	6%
Program B	29%	41%	24%	4%	2%

Regarding storing passwords securely in both programs, 36% believe that a password is stored securely in program A compared to 80% for program B. These findings show that the majority of participants believe that a password is stored securely in program B which implies that allowing participants to store passwords in a preferred location, and showing them the password in an encrypted form, will reassure them about the strong security of the system.

Table 7.14: Password is stored securely in it.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	9%	27%	29%	25%	10%
Program B	28%	52%	13%	4%	3%

For the final question in this section, I found that only 28% of participants trust program A to not synchronize passwords compared to 69% who trust program B. Thus, the results prove that allowing participants to decide about synchronizing each password at the stage of adding it to the system can increase their trust, also participants can see that a password is only stored in their chosen location along with the date and time.

Table 7.15: I trust it to not synchronize my passwords over different devices (e.g., computers, smartphones) without my permission.

Programs	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Program A	7%	21%	34%	26%	12%
Program B	23%	46%	25%	3%	3%

So, based on the findings from these questions about program A and program B, I found that improving transparency and control in password managers lead to a better understanding of the system along with enhancing trust in password managers.

In addition, to determine if there are any significant differences between program A and program B in the 11 questions, I used a Wilcoxon Signed-Ranks test (Table 7.16). I found that there were significant differences between program A and program B in answer to all 11 questions. The findings confirm the hypotheses: (1) improving transparency in password managers leads to a better understanding of the system, and (2) it enhances trust in password managers.

For example, a Wilcoxon signed-rank test shows that participants know where passwords are stored in program B (median = 4.0) more than in program A (median = 3.0) and the difference is significant, ($Z = -3.725, p < .001$). Likewise, a Wilcoxon signed-rank test indicates that participants trust program B (median = 4.0) to store all passwords more than program A (median = 3.0) and the difference is significant, ($Z = -5.416, p < .001$).

Table 7.16: Comparing between program A and program B using a Wilcoxon Signed-Ranks test. The table shows the mean (average) and median, Z score and p-value of each statement.

	Statements	Mean & (Med.) of A	Mean & (Med.) of B	Z score	p-value .05
1	I know where my online passwords are stored.	2.97 (3.0)	3.93 (4.0)	-3.725	Sig $p < .001$
2	I fully understand how my passwords are processed.	3.24 (3.50)	3.96 (4.0)	-3.532	Sig $p < .001$
3	I understand how it works.	3.47 (4.0)	3.88 (4.0)	-2.416	Sig $p < .016$
4	I understand how it generates the encryption key.	2.78 (3.0)	3.87 (4.0)	-4.932	Sig $p < .001$
5	I understand the benefit of a random password generator.	3.65 (4.0)	4.15 (4.0)	-2.875	Sig $p < .004$
6	I trust it to store all my online passwords.	2.85 (3.0)	3.94 (4.0)	-5.416	Sig $p < .001$
7	I trust it to delete my password from its database permanently after I have deleted it from my account.	3.06 (3.0)	3.88 (4.0)	-4.783	Sig $p < .001$
8	I trust it to generate a strong key to encrypt my password.	2.71 (3.0)	4.16 (4.0)	-5.893	Sig $p < .001$
9	I feel that I have control of my passwords when I store them.	3.09 (3.0)	3.93 (4.0)	-4.052	Sig $p < .001$
10	Password is stored securely.	2.99 (3.0)	3.97 (4.0)	-4.806	Sig $p < .001$
11	I trust it to not synchronize my passwords over different devices without my permission.	2.85 (3.0)	3.84 (4.0)	-4.942	Sig $p < .001$

7.4.2 Features of Program B

After the 68 participants answered a set of questions about program A and B, I asked them which program do they prefer. I found that 75% of participants (69% of users and 81% of non-users) preferred program B compared to 25% of participants who preferred program A. Regarding the 75% of participants who preferred program B, I asked them a set of questions about the importance of factors and the advantages of program B. As seen in table 7.17, I found that 92% of participants found the text box in program B very

important / important, while 88% of participants found preventing/ allowing password synchronization very important / important.

Also, 84% believed that choosing the location to store passwords is very important / important, while 98% of participants rated generating a key to encrypt each password as very important / important. We can see that the features provided in program B were rated very important / important by the majority of the 51 participants as the lowest percentage is for the coloured and visible buttons (74%) and showing the stored password in an encrypted form (78%).

Table 7.17: 51 Participants answered 9 questions about the importance of each feature/ factor of program B. The range is from not important at all to very important.

	Questions	Not impor- tant at all	Slightly important	Important	Very im- portant
1	I can choose a place to store passwords.	4%	12%	29%	55%
2	It shows me the location of stored passwords.	6%	14%	35%	45%
3	I can generate an encryption key to encrypt each password.	2%	0%	33%	65%
4	It shows me the encryption key that is used to encrypt passwords.	2%	16%	39%	43%
5	I can prevent/allow password synchronization for each password.	2%	10%	43%	45%
6	It shows me the stored password in an encrypted form.	8%	14%	47%	31%
7	It shows me the date and time when the password was last stored.	4%	16%	31%	49%
8	The buttons in program B are coloured and are visible.	10%	16%	47%	27%
9	The text boxes that explain features such as the benefit of password generator.	4%	4%	51%	41%

In regard to the 25% of participants (31% of users and 19% of non-users) who pre-

ferred program A over B; many of them stated different reasons. Program A is easy and simple to use, and some participants found it familiar as it is similar to current password managers. Other participant found program B complicated (table 7.18).

Table 7.18: Comments by participants about preferring program A over program B.

Code	Sample of comments
Easy and simple	<ul style="list-style-type: none"> • Less complicated options, faster and easier to use. • It is a lot simpler to use and there is too much choice in B. All I want is for the program to store the passwords and I don't really care how it works but it does. • Program A is easier to use and faster.
Familiar program	<ul style="list-style-type: none"> • A is more similar to what I have used before. • Because they are more common.

7.4.3 Usability of Program B

All 68 participants answered ten questions on a System Usability Scale (SUS) about program B (Table 7.19). I found that the SUS score for all types is 66.03 which implies that program B is a marginal high acceptable program which is closer to the rate "Good". All participants' answers to SUS questions can be found in table 7.20.

Table 7.19: System Usability Scale (SUS) Score.

Type of participants	Average SUS score
All 68 participants	66.03
31 Experts	70.56
37 Non-experts	62.23
36 Users	67.01
32 Non-users	64.92
31 Laptop/desktop users	66.29
37 Smartphone users	65.81

I also compare the SUS scores between other groups of participants (experts and non-experts, users and non-users, desktop and smartphones). The SUS score for experts is 70.56, while the SUS score for non-experts is 62.23. So, experts found program B usable

compared to non-experts because non-experts might need help from a technical person to use program B, while experts are familiar with programs. In regard to users and non-users, the SUS score for users is 67.01 while the score is 64.92 for non-users. For participants who use a desktop/ laptop or a smartphone, the SUS score for desktop/laptop users is 66.29 while it is 65.81 for smartphone users which are very similar to each other.

Table 7.20: SUS questions were answered by 68 participants about program B.

	Questions	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	I think that I would like to use this system frequently.	22%	50%	16%	12%	0%
2	I found the system unnecessarily complex.	6%	16%	25%	46%	7%
3	I thought the system was easy to use.	24%	51%	13%	10%	2%
4	I think that I would need the support of a technical person to be able to use this system.	6%	15%	7%	41%	31%
5	I found the various functions in this system were well integrated.	15%	53%	31%	1%	0%
6	I thought there was too much inconsistency in this system.	1%	9%	28%	46%	16%
7	I would imagine that most people would learn to use this system very quickly.	15%	53%	25%	7%	0%
8	I found the system very cumbersome to use.	2%	25%	29%	31%	13%
9	I felt very confident using the system.	15%	60%	21%	3%	1%
10	I needed to learn a lot of things before I could get going with this system.	10%	16%	22%	37%	15%

In regard to the language used for program B, I found that 52% of participants are satisfied, 35% of participants are very satisfied while only 13% are neither satisfied nor

dissatisfied. For the design of program B, I found that 30% of participants found the design excellent, 41% found it good, 19% found it average, while 7% of participants found the design fair and only 3% found it poor.

Furthermore, I asked the participants two open-ended questions about the things they like and dislike about program B. The comments from the two questions were analyzed qualitatively using inductive coding. The things participants liked the most are that program B is trustworthy and secure, a transparent tool and informative (table 7.21). On the other hand, the things that participants disliked most in program B are that the user interface of the program is not flexible, the program is not user friendly and there is a security concern about stored passwords (table 7.22).

Table 7.21: Comments sample about the things they like most in program B.

Code	Sample of comments
Trustworthy and secure	<ul style="list-style-type: none"> • User trust and confidence are attained by program B. • More secure and organised . • I do not have to worry about thinking about a password, the password is generated for me and it is very safe, I can see the location and I can trust saving this password and I know where it is being stored.
Transparent tool	<ul style="list-style-type: none"> • It shows me how and where passwords stored. • The "low-level" access to important password data, specifically encryption type, encrypted form and data storage location. • My preference was program A, but I like the concept of transparency when it comes to password managers.
Informative	<ul style="list-style-type: none"> • Encryption key and hovering over the i to get a bit more understanding of each section. • Help text and description for each field in the form. Also the overview which explains how the program works overall. • I liked the links to explain things further that did not have enough information provided on the page.
More choices	<ul style="list-style-type: none"> • Give me choices.

Table 7.22: Comments sample about the things they dislike most in program B.

Code	Sample of comments
User interface not flexible	<ul style="list-style-type: none"> • GUI can be improved and more details should be added. • Need a more modern touch / more css maybe with better styling.
Not user friendly	<ul style="list-style-type: none"> • The long process. • It is complex. I don't know how to use it if I don't have enough knowledge about cryptography. • The implied responsibility on the user (to maintain the key - step 2). Password managers are suppose to reduce the cognitive burden not increase.
Security concern	<ul style="list-style-type: none"> • Relatively could be revealing hint of location where passwords are kept geographically malicious attackers to pursue.

Finally, some participants provided a few comments at the end of the study in regard to program B. A participant said that it is an important study as increasing transparency is vital as the use of this technology progresses and an individual ability to protect their data is equally vital. Another participant said a password manager is convenient but people do not know how it is running which could fail to be trusted. So, these comments show that the idea of improving transparency in password managers can be a promising solution to trust and transparency issues.

7.5 Discussion

In the extended study, I found that most participants know where passwords are stored in program B compared to program A. Most of them understand how passwords are processed in program B and how things work compared to program A. Importantly, more participants trust program B to store all their passwords, delete them permanently, store passwords securely and not synchronize them without permission. Statistically, I found that there were significant differences between program A and program B in 11 questions which confirmed the hypotheses: (1) improving transparency and control lead to a better

understanding of the system, and (2) enhance trust in password managers.

So, the findings of this study prove and confirm the findings from the previous study which shows that allowing participants to be involved in many steps can be a strong way to solve trust, security and transparency issues in password managers. The trust and transparency issues and security concerns were the main reasons for not using password managers (section 4.3.2 and 5.3.1), while users of password managers have similar trust issue and security concern (section 4.3.2 and 5.3.2).

Moreover, by allowing people to be involved in encrypting a password and showing the encrypted password, it can overcome security concerns with password managers. Also, providing more details and different suitable colours within the program can increase awareness and understanding of how the system works for the end users, for example, providing different colours for buttons like delete and details in program B.

The new findings in this study are that 75% of participants (69% of users and 81% of non-users) preferred program B over program A. The results show that the provided features that improve transparency in program B are important to participants such as choosing and showing the place of stored passwords, generating and showing the encryption keys, preventing/allowing password synchronization and showing the date and time of stored passwords. In addition, the vast majority of participants who preferred program B found the coloured buttons and text boxes are important.

The overall SUS score for program B is 66.03, which is a marginal high acceptable. The most liked things about program B are that it is transparent and trustworthy (table 7.21), while the most disliked things in the program are that the user interface is not flexible and it is not user friendly (table 7.22). Lastly, some participants preferred program A over program B because it is easy and simple to use and less complicated.

7.5.1 Recommendations for Improving Password Managers

Based on the findings in the two user studies, I recommend the following:

(1.) Password managers should allow users to choose the place to store a password and provide many options, such as storing a password on one's own device, in cloud storage (e.g., Google drive) or on a password manager server. Importantly, users should know the location of a stored password.

(2.) Password managers should allow users to choose which device to synchronize passwords to. For example, users might only want to synchronize a few passwords for shopping websites, but they might prefer not to synchronize passwords for financial accounts and only want to store them on a specific device.

(3.) Password managers should allow users to customize their own password manager. For example, a user may want to be involved in each step such as choosing a location to store passwords, generate encryption keys and allow synchronization. On the other hand, another user may only want to choose the location to store passwords and nothing else. Also, users should be able to choose what kind of details they want to see, such as encryption keys, date and time and place of stored passwords.

(4.) Password managers should give more details about how it works and manages passwords. Useful information should be included to educate users about different things, such as the benefits of a random generator and protect passwords against identity theft.

(5.) Password managers should consider non-technical users in regard to using the tool and the language used. Users with a technical background might not have problems using password managers and understanding the language used (computer jargon), but non-technical users could have problems. Password managers should include two views, one for non-technical users and another for technical users.

(6.) The second study shows that visible and coloured buttons are an important feature in the program. So, password managers should make the buttons visible and coloured.

7.6 Conclusion

The results of the extended study proved and confirmed the results of the previous study (chapter 6). The majority of participants knew where passwords are stored and how they are processed in program B compared to program A. Likewise, more participants trust program B to store passwords and delete them permanently compared to program A. Interestingly, 75% of participants preferred program B over program A, and there were significant differences between program B and program A in all questions which proved and confirmed the hypotheses.

Finally, the recommendations are that password managers should allow users to choose the location to store passwords, allow them to customize their own password managers and give more details within the program.

Chapter 8

Discussion and Conclusion

8.1 Summary

Technology has become an essential part in our daily life, but relying on technology has created privacy concerns in regard to people's data which is protected by passwords. Passwords are required by websites for authentication and the actual fact is that passwords are simple and easy to use but they are very important to protect personal accounts and data. The problem is that people find it difficult to memorize multiple passwords for their accounts, especially if passwords are random, long and strong. Thus, they use insecure practices such as password reuse and including personal information within passwords. Therefore, solutions were proposed to solve these problems and help people manage their own passwords safely, such as password strength meter and a password policy.

The proposed solutions can help people to create strong and long passwords, yet, these solutions do not help people to memorize multiple passwords or store passwords for them. Thus, another solution is a password manager which can generate a random password for an account, store it and remember it for people as well. Password managers can be a solution to help people handle their own passwords properly, but they have some issues.

Researchers stated that there are security flaws in password managers and it does not solve password reuse problem. Also, people have a lack of trust in the program, they have a lack of understanding its benefit and they view password managers as a security risk. Thus, researchers proposed and suggested solutions to solve these problems with pass-

word managers such as [9], [15], [16], [91], while others called for further investigation [78], [81], [85]. However, previous studies predominately focused on passwords or on the technical and security side of password managers, but less on the human perception and usability and user interface of password managers.

Consequently, I concentrated on the user interfaces and usability of password managers as well as the human perspective (users and non-users) in password managers. I conducted different studies where I analyzed the user interfaces and usability of cloud password managers, data from users of password managers; and I gained insights into why non-users do not use these tools. I also conducted a user study with users and non-users of password managers to understand, in depth, their thoughts about password managers.

8.2 Discussion

In the evaluation of three password managers using Nielsen's principles (section 3.3.1), I found that cloud password managers have a consistent design, provide concrete icons and terminology while a user can store personal information and multiple online passwords. The current cloud password managers offer autofill feature for credentials to login, they provide a built-in password generator and help section to guide users. These features are very useful because the user can generate a random password for each account, store it and use the autofill feature to fill in the username and password which saves time.

In the user study of LastPass (section 4.3.1), the results show that there were no significant differences between users and non-users when using a cloud-based password manager (LastPass), 40% of participants found it easy to use LastPass, while 47% were neutral about it. Actually, most of them found it easy to create an account, store and access passwords, even though 29 participants used it for the first time. Plus, 46% of participants found the design of LastPass average. Similarly, the results of the questionnaire study (section 5.3.2) show that users of password managers found it easy to use, store and access passwords as well as many of them found it easy to use password managers on

multiple devices. Overall, current password managers offer many features and are easy to use and users can familiarise themselves with them after using them for a few times.

However, based on the findings of the heuristic evaluation study (section 3.3.2), cloud password managers should avoid using computer jargon and should reduce the complexity of their system design because the more features they have, the more complex they become. So, they can be easier to use and adopted by more people particularly novices. Cloud password managers should facilitate the process of recovering an account in case a user forgets the master password. Also, a few participants in the user study (section 4.3.1) did not like the colour and design, they found LastPass not user friendly and the process to recover the account is strict/difficult. Likewise, a few users of password managers such as LastPass and 1Password in the questionnaire study (section 5.3.2) found it difficult to recover the account, while others found it hard to use the programs on multiple devices.

By looking at the findings in user study (section 4.3.1) and the heuristic evaluation study (section 3.3.2), I found similarities between participants' answers and the findings in heuristic study. I believe that the result of the users study is generally applicable for other password managers. Participants stated things that are similar to the one I found during the heuristic evaluation, for example, they do not like the account setting colour of LastPass, no asterisks for mandatory fields and LastPass does not have a strong master password policy. Also, participants found it easy to store and access passwords in LastPass (section 4.3.1), which is similar to the finding in the questionnaire study (section 5.3.2) as users of many password managers found it easy. Likewise, some users of password managers in the questionnaire study found it hard to recover the account which is similar to participants' answers in the user study about LastPass.

Based on the comments and answers from participants in the user study and the findings in the heuristic study, I suggest a better design of cloud password managers for all users, which is in line with [78], also, I suggest less use of computer jargon and reducing the features in password managers, leaving options for users to add. I 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 as well as not all features being free. This finding about the use of Chrome was suggested by Stobert and Biddle [13], as they called for integrating password managers into browsers.

In addition, most users of password managers (section 5.3.2) 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 user study (section 4.3.1), where most users used password managers to store passwords and for ease of access. These findings suggest that users in both studies do not use other features of password managers or they might not be interested in them. Regarding random password generators, half of the users in the questionnaire study and the vast majority of participants in the user 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. However, many users of LastPass and 1Password password managers use random password generators which shows that cloud-based password managers can help to reduce password reuse.

Moreover, I found that having an education related to computer science or information security does not necessarily increase the adoption of password managers. Plus, I found no significant differences between experts and non-experts when they are using password managers, while I found only two differences between expert and non-expert non-users for the reasons that they do not use password managers. So, education does not play a significant role when using or not using password managers, which I assume it is related to people's view about these tools. In contrast, I found that education is an important factor as experts have more passwords than non-experts, yet, experts still reuse passwords, which was found in [13], [55]. Furthermore, users in the questionnaire and user study reuse password which was also found in [46], [47], [81].

Furthermore, I 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 5.3.1), followed by reasons that related to trans-

parency and security. I also found that all non-users in the user study (section 4.3.2) did not trust the vendor of password managers to store passwords or delete them permanently. Thus, non-user participants in both studies do not trust the vendors of password managers to store passwords or delete them permanently. So, trust is the main reason why non-users do 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 most of non-users in the user study and non-users in the questionnaire study did not know where passwords are stored nor the process of storing passwords. Likewise, security concerns about the databases of password managers and master passwords are another important reason that makes non-user participants not to use password managers. The security concern finding is in line with the study [40], [83], [86]. However, the low adoption rate for password managers is mainly due to trust and transparency issues, and security concerns. A small number of non-user participants are not aware of password managers, while some non-users do not use password managers due to usability issues which is in line with [83].

Besides, most users of different types of password managers (section 5.3.2) have security concerns about master passwords as well as worrying about losing their stored passwords in password managers. Their worries about master passwords are justified, because in the heuristic evaluation study (section 3.3.2), I found that the current policy for master passwords in password managers, particularly LastPass and 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 user study (section 4.3.2) stated that the master password policy in LastPass is weak and so it should apply special characters and have a strong and strict policy. So, password managers must use a strong policy for a master password which is in line with study [9].

Additionally, I discovered that around half of users in the questionnaire study and the majority of users in the user study have trust issues towards the vendors of password managers, and so most of them do not store all their passwords. Similarly, many users in both studies have a transparency issue towards password managers regarding the location of stored passwords, and the process as well. These findings answer the question on whether many users have trust issues and security concerns. Thus, based on the results, they imply that 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.

Regarding the accepting and adoption of password managers, the results of the studies show that number of non-users did not use password managers because they were not aware of them, which suggests that they did not reach the first stage of the adoption life cycle which is the awareness stage. Based on the results, the low adoption of password managers is not mainly due to lack of awareness, but because of trust issues, followed by lack of transparency and security concerns, while usability is only a minor issue. Thus, I assume that many non-users reached the first stage and they were aware of the existence of password managers, but they might decide not to adopt the programs in other stages. I assume that some non-users might decide not to use password managers in the interest stage, others might decide not to adopt the programs in the evaluation and trial stages, but none of non-users reached the adoption stage because they do not use password managers.

For users of password managers, they reached all stages of the adoption life cycle because they are using password managers. The findings indicate that although some users accepted and adopted password managers and found the programs easy to use and useful, they still have trust issues and security concerns similar to non-users who decided not to adopt password managers. In regard to the educational background, more expert participants adopted password managers compared to non-expert participants, so we can see that expert participants were more aware of password managers, but the difference

is not significant. Also, expert users were more aware of cloud-based and open-source password managers compared to non-expert users, which implies that expert users have better awareness and interest in different types of password managers compared to non-expert users.

To solve the problem with trust and transparency issues in password managers, I designed a prototype and conducted two user studies about improving transparency in password managers in which I used participants' answers to test the hypothesis. I found that the majority of participants know where passwords are stored in a transparent manager/program B, understand how passwords are processed and how the program works compared to a non-transparent manager/program A. Likewise, more participants trust a transparent manager/program B to store all passwords, delete them permanently and store passwords securely compared to non-transparent/program A.

Importantly, non-user participants became more willing to adopt a password manager if it was the same as a transparent manager, while 75% of participants (69% of users and 81% of non-users) in the extended user study preferred program B because of the features it offers. Statistically, there were significant differences between the programs (non-transparent/program A vs. transparent/program B) in all questions, which prove and confirm the hypothesis which is that improving transparency in password managers leads to a better understanding of the system and enhances trust in password managers.

Therefore, I found that improving transparency and allowing people to be involved in many steps while adding a password and storing it can be helpful to bridge the trust gap and solve the trust issue in password managers. It will increase their awareness and understanding of how password managers work. Also, by allowing people to encrypt and decrypt a password and show an encrypted password on a screen can overcome security concerns with password managers.

The findings from the two user studies (sections 6.4.1 and 7.4.1) come in line with a recent study by Ray *et al.* [90], who suggested that a higher level of transparency could

help to increase the level of trust among users by showing how secure the passwords are when they are stored in password managers. It was also stated in study [83]; the decision to adopt applications (password managers) can be influenced by transparency which explains how the system manages data. Moreover, providing information regarding how password managers protect and store passwords might provide non-expert users more understanding about the benefits and risks of password managers [78].

Based on the findings from the two user studies, I recommend that password managers should allow users to choose the location where they store a password and provide them with additional storage location options. Password managers should allow users to choose which passwords and device to synchronize, and users should be allowed to customize their own password manager, for example, users can be involved in each step such as choosing a location to store passwords or only generate an encryption key for each password. Also, password managers should give more details within the program such as how it works, so they educate users about the program, as well as consider non-technical users in regard to using the tool, the language used and provide them with more details.

Finally, a password generator should have visible buttons placed around the password form to make it easy to reach them and encourage people to use them as well as they should produce memorable and strong passwords, which will help mitigate weak password and password reuse. I believe that educating people is very important to increase their understanding about the benefits of password generators and password managers, which is similar to Pearman *et al.* who called for more focus on non-experts [78].

8.3 Research Findings and Contributions

The main findings and contributions of this thesis as follows:

- Investigating the user interface and usability of three cloud password managers (LastPass, Dashlane and Keeper) using Nielsen's 10 principles. The investigation

was useful and helpful because I found and identified a few issues in the user interface and in the usability of the programs as well as suggested recommendations to solve these problems. Furthermore, the findings of the investigation show that current cloud password managers offer many features such as storing passwords, storing personal information and fill in username and password on behalf of user.

- A user study with group of participants in order to understand how users and non-users of password managers find it in terms of usability and trust. The user study was helpful to find, in depth, how users and non-users found a cloud password manager and their views of password managers in general. The findings show that there are similarities between users and non-users in many aspects such as ease of use and satisfaction in regard to LastPass, while users and non-users have a lack of trust and transparency issues towards password managers.
- The online questionnaire study was conducted with users and non-users of password managers as well as experts and non-experts. The findings show that non-users do not use password managers because of lack of trust and transparency and security concerns. Similarly, many users have trust and transparency issues and security concerns towards password managers, but they found it easy to use.
- A multi-platform prototype was built and distributed online in order to answer the hypotheses about improving transparency in password managers. The findings from participants' answers from two user studies show that the program (prototype) is highly acceptable in terms of usability. Importantly, the user studies show and prove that improving transparency in password managers leads to a better understanding of the system and enhances trust in password managers. Also, it makes non-users more willing to adopt a password manager if it is the same as a transparent manager, as well as the majority of participants preferred program B in the second study.

8.4 Future Work

For heuristics evaluation (chapter 3), I evaluated three password managers by myself using Nielsen's 10 principles, so researchers who are interested in usability and designing can expand the evaluation of password managers using more evaluators (experts) as well as apply other heuristics such as Schneiderman's 8 golden rules. For the user study (chapter 4), I only measured the usability of LastPass, so it is a good idea to conduct a long-term study to evaluate learnability. Also, doing a pre-test before starting the user study can be useful and helpful.

Moreover, the idea of transparency (chapter 6 and 7) can be expanded to include more security options. Security researchers could apply their ideas such as adding more options for the length of encryption keys, offering different types of encryption algorithms, and providing hashing algorithm options such as SHA-256. Moreover, researchers who are interested in smartphones can apply the idea of transparency on smartphone applications for password managers, provide more guidance for smartphone users, and they can explore different aspects such as usability.

8.5 Conclusion

In this research, I concentrated on users and non-users of password managers in different aspects such as usability and trust. I also evaluated the user interface and usability of three password managers using Nielsen's 10 principles. The findings from these studies show that there are trust issues and lack of transparency towards password managers, while usability is only a small issue. Therefore, I designed a prototype of a transparent manager and evaluated the prototype using answers from participants, which showed that improving transparency can be a promising solution as it can enhance trust between people and password managers and can lead to a better understanding of password managers.

Bibliography

- [1] S. T. Haque, M. Wright, and S. Scielzo, “A study of user password strategy for multiple accounts”, in *Proceedings of the Third ACM Conference on Data and Application Security and Privacy*, ser. CODASPY ’13, San Antonio, Texas, USA: Association for Computing Machinery, 2013, 173–176, ISBN: 9781450318907. DOI: 10.1145/2435349.2435373.
- [2] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “Passwords and the evolution of imperfect authentication”, *Commun. ACM*, vol. 58, no. 7, 78–87, Jun. 2015, ISSN: 0001-0782. DOI: 10.1145/2699390.
- [3] M. Kotadia. (2004). Gates predicts death of the password, [Online]. Available: <https://www.cnet.com/news/gates-predicts-death-of-the-password> (visited on May 2020).
- [4] IBM. (2011). Ibm reveals five innovations that will change our lives in the next five years (update), [Online]. Available: <https://phys.org/news/2011-12-ibm-reveals-years.html> (visited on May 2020).
- [5] S. Chaudhary, T. Schafeitel-Tähtinen, M. Helenius, and E. Berki, “Usability, security and trust in password managers: A quest for user-centric properties and features”, *Computer Science Review*, vol. 33, pp. 69–90, 2019, ISSN: 1574-0137. DOI: <https://doi.org/10.1016/j.cosrev.2019.03.002>.

-
- [6] F. Al Maqbali and C. J. Mitchell, “Autopass: An automatic password generator”, in *2017 International Carnahan Conference on Security Technology (ICCST)*, 2017, pp. 1–6. DOI: 10.1109/CCST.2017.8167791.
- [7] R. Zhao and C. Yue, “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*, ser. CODASPY ’13, San Antonio, Texas, USA: Association for Computing Machinery, 2013, 333–340, ISBN: 9781450318907. DOI: 10.1145/2435349.2435397.
- [8] Y. Li, H. Wang, and K. Sun, “A study of personal information in human-chosen passwords and its security implications”, in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, 2016, pp. 1–9. DOI: 10.1109/INFOCOM.2016.7524583.
- [9] C. Luevanos, J. Elizarraras, K. Hirschi, and J.-h. Yeh, “Analysis on the security and use of password managers”, in *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, 2017, pp. 17–24. DOI: 10.1109/PDCAT.2017.00013.
- [10] D. Florêncio, C. Herley, and P. C. van Oorschot, “Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts”, in *23rd USENIX Security Symposium (USENIX Security 14)*, San Diego, CA: USENIX Association, Aug. 2014, pp. 575–590, ISBN: 978-1-931971-15-7. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/florencio>.
- [11] M. Golla and M. Dürmuth, “On the accuracy of password strength meters”, in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’18, Toronto, Canada: Association for Computing Machinery, 2018, 1567–1582, ISBN: 9781450356930. DOI: 10.1145/3243734.3243769.

-
- [12] H. Habib, P. E. Naeini, S. Devlin, M. Oates, C. Swoopes, L. Bauer, N. Christin, and L. F. Cranor, “User behaviors and attitudes under password expiration policies”, in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, Baltimore, MD: USENIX Association, Aug. 2018, pp. 13–30, ISBN: 978-1-939133-10-6. [Online]. Available: <https://www.usenix.org/conference/soups2018/presentation/habib-password>.
- [13] E. Stobert and R. Biddle, “The password life cycle”, *ACM Trans. Priv. Secur.*, vol. 21, no. 3, 2018, ISSN: 2471-2566. DOI: 10.1145/3183341.
- [14] E. Stobert and R. Biddle, “A password manager that doesn’t remember passwords”, in *Proceedings of the 2014 New Security Paradigms Workshop*, ser. NSPW ’14, Victoria, British Columbia, Canada: Association for Computing Machinery, 2014, 39–52, ISBN: 9781450330626. DOI: 10.1145/2683467.2683471.
- [15] D. McCarney, D. Barrera, J. Clark, S. Chiasson, and P. C. van Oorschot, “Tapas: Design, implementation, and usability evaluation of a password manager”, in *Proceedings of the 28th Annual Computer Security Applications Conference*, ser. ACSAC ’12, Orlando, Florida, USA: Association for Computing Machinery, 2012, 89–98, ISBN: 9781450313124. DOI: 10.1145/2420950.2420964.
- [16] Y. Li, H. Wang, and K. Sun, “Bluepass: A secure hand-free password manager”, in *Security and Privacy in Communication Networks*, X. Lin, A. Ghorbani, K. Ren, S. Zhu, and A. Zhang, Eds., vol. 238, Cham: Springer, 2018, pp. 185–205, ISBN: 978-3-319-78813-5. DOI: https://doi.org/10.1007/978-3-319-78813-5_10.
- [17] Z. Li, W. He, D. Akhawe, and D. Song, “The emperor’s new password manager: Security analysis of web-based password managers”, in *23rd USENIX Security Symposium (USENIX Security 14)*, San Diego, CA: USENIX Association, Aug. 2014, pp. 465–479, ISBN: 978-1-931971-15-7. [Online]. Available: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/li_zhiwei.

-
- [18] Y.-T. Liu, D. Du, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, and Z. Liang, “Splitpass: A mutually distrusting two-party password manager”, *Journal of Computer Science and Technology*, vol. 33, pp. 98–115, 2018. DOI: <https://doi.org/10.1007/s11390-018-1810-y>.
- [19] R. Zhao, C. Yue, and K. Sun, “Vulnerability and risk analysis of two commercial browser and cloud based password managers”, *ASE Science Journal*, vol. 1, no. 4, pp. 1–15, 2013.
- [20] P. Gasti and K. B. Rasmussen, “On the security of password manager database formats”, in *Computer Security – ESORICS 2012*, S. Foresti, M. Yung, and F. Martinelli, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 770–787, ISBN: 978-3-642-33167-1. DOI: https://doi.org/10.1007/978-3-642-33167-1_44.
- [21] B. Yang, H. Chu, G. Li, S. Petrovic, and C. Busch, “Cloud password manager using privacy-preserved biometrics”, in *2014 IEEE International Conference on Cloud Engineering*, 2014, pp. 505–509. DOI: 10.1109/IC2E.2014.91.
- [22] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, “Password managers: Attacks and defenses”, in *23rd USENIX Security Symposium (USENIX Security 14)*, San Diego, CA: USENIX Association, Aug. 2014, pp. 449–464, ISBN: 978-1-931971-15-7. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/silver>.
- [23] Cambridge. (2022). Meaning of trust in english, [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/trust> (visited on May 2022).
- [24] Cambridge.. (2022). Meaning of transparency in english, [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/transparency> (visited on May 2022).

-
- [25] Cambridge. (2022). Meaning of adoption in english, [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/adoption> (visited on May 2022).
- [26] Dictionary. (2022). Adoption definition and meaning, [Online]. Available: <https://www.dictionary.com/browse/adoption> (visited on May 2022).
- [27] Cambridge. (2022). Meaning of security in english, [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/security> (visited on May 2022).
- [28] J. Nielsen. (1994). 10 usability heuristics for user interface design, [Online]. Available: www.nngroup.com/articles/ten-usability-heuristics (visited on Jul. 2020).
- [29] D. Pierotti and J. Nielsen. (2012). Xerox/nielsen 13 usability heuristics, [Online]. Available: <https://uxmanager.net/heuristics/xeroxnielsen-13-usability-heuristics> (visited on Jul. 2020).
- [30] L. Lamport, “Password authentication with insecure communication”, *Commun. ACM*, vol. 24, no. 11, 770–772, Nov. 1981, ISSN: 0001-0782. DOI: 10.1145/358790.358797.
- [31] M. A. Sasse, S. Brostoff, and D. Weirich, “Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security”, *BT technology journal*, vol. 19, no. 3, pp. 122–131, 2001. DOI: <https://doi.org/10.1023/A:1011902718709>.
- [32] B. Meyer. (2021). Comb: Largest breach of all time leaked online with 3.2 billion records, [Online]. Available: <https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free/> (visited on Mar. 2021).
- [33] V. Zimmermann and N. Gerber, “The password is dead, long live the password – a laboratory study on user perceptions of authentication schemes”, *International*

-
- Journal of Human-Computer Studies*, vol. 133, pp. 26–44, 2020, ISSN: 1071-5819. DOI: <https://doi.org/10.1016/j.ijhcs.2019.08.006>.
- [34] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, ““i added ’!’ at the end to make it secure”: Observing password creation in the lab”, in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, Ottawa: USENIX Association, Jul. 2015, pp. 123–140, ISBN: 978-1-931971-249. [Online]. Available: <https://www.usenix.org/conference/soups2015/proceedings/presentation/ur>.
- [35] N. Woods and M. Siponen, “Improving password memorability, while not inconveniencing the user”, *International Journal of Human-Computer Studies*, vol. 128, pp. 61–71, 2019, ISSN: 1071-5819. DOI: <https://doi.org/10.1016/j.ijhcs.2019.02.003>.
- [36] N. Woods and M. Siponen, “Too many passwords? how understanding our memory can increase password memorability”, *International Journal of Human-Computer Studies*, vol. 111, pp. 36–48, 2018, ISSN: 1071-5819. DOI: <https://doi.org/10.1016/j.ijhcs.2017.11.002>.
- [37] M. AlSabah, G. Oligeri, and R. Riley, “Your culture is in your password: An analysis of a demographically-diverse password dataset”, *Computers and Security*, vol. 77, pp. 427–441, 2018, ISSN: 0167-4048. DOI: <https://doi.org/10.1016/j.cose.2018.03.014>.
- [38] H. Petrie and B. Merdenyan, “Cultural and gender differences in password behaviors: Evidence from china, turkey and the uk”, in *Proceedings of the 9th Nordic Conference on Human-Computer Interaction*, ser. NordiCHI ’16, Gothenburg, Sweden: Association for Computing Machinery, 2016, ISBN: 9781450347631. DOI: [10.1145/2971485.2971563](https://doi.org/10.1145/2971485.2971563).
- [39] M. Grobler, M. Chamikara, J. Abbott, J. J. Jeong, S. Nepal, and C. Paris, “The importance of social identity on password formulations”, *Personal and Ubiquitous*

-
- Computing*, vol. 25, no. 5, pp. 813–827, 2021. DOI: <https://doi.org/10.1007/s00779-020-01477-1>.
- [40] X. Gao, Y. Yang, C. Liu, C. Mitropoulos, J. Lindqvist, and A. Oulasvirta, “Forgetting of passwords: Ecological theory and data”, in *27th USENIX Security Symposium (USENIX Security 18)*, Baltimore, MD: USENIX Association, Aug. 2018, pp. 221–238, ISBN: 978-1-939133-04-5. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity18/presentation/gao-xianyi>.
- [41] M. Ciampa, “A comparison of password feedback mechanisms and their impact on password entropy”, *Information Management & Computer Security*, vol. 21(5), pp. 344–359, 2013. DOI: 10.1108/IMCS-12-2012-0072.
- [42] B. Brumen and T. Makari, “Resilience of students’ passwords against attacks”, in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2017, pp. 1275–1279. DOI: 10.23919/MIPRO.2017.7973619.
- [43] C. Shen, T. Yu, H. Xu, G. Yang, and X. Guan, “User practice in password security: An empirical study of real-life passwords in the wild”, *Computers & Security*, vol. 61, pp. 130–141, 2016, ISSN: 0167-4048. DOI: <https://doi.org/10.1016/j.cose.2016.05.007>.
- [44] B. Ives, K. R. Walsh, and H. Schneider, “The domino effect of password reuse”, *Communications of the ACM*, vol. 47, no. 4, pp. 75–78, 2004.
- [45] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, “Do users’ perceptions of password security match reality?”, in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’16, San Jose, California, USA: Association for Computing Machinery, 2016, 3748–3760, ISBN: 9781450333627. DOI: 10.1145/2858036.2858546.
- [46] R. Wash, E. Rader, R. Berman, and Z. Wellmer, “Understanding password choices: How frequently entered passwords are re-used across websites”, in *Twelfth Sym-*

-
- posium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO: USENIX Association, Jun. 2016, pp. 175–188, ISBN: 978-1-931971-31-7. [Online]. Available: <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/wash>.
- [47] S. Pearman, J. Thomas, P. E. Naeini, H. Habib, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, and A. Forget, “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*, ser. CCS ’17, Dallas, Texas, USA: Association for Computing Machinery, 2017, 295–310, ISBN: 9781450349468. DOI: 10.1145/3133956.3133973.
- [48] Ponemon. (2019). 2019 state of password and authentication security behaviors report, [Online]. Available: <https://pages.yubico.com/2019-password-and-authentication-report> (visited on Mar. 2021).
- [49] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, “Encountering stronger password requirements: User attitudes and behaviors”, in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ser. SOUPS ’10, Redmond, Washington, USA: Association for Computing Machinery, 2010, ISBN: 9781450302647. DOI: 10.1145/1837110.1837113.
- [50] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, “Does my password go up to eleven? the impact of password meters on password selection”, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI ’13, Paris, France: Association for Computing Machinery, 2013, 2379–2388, ISBN: 9781450318990. DOI: 10.1145/2470654.2481329.
- [51] P. Poornachandran, M Nithun, S. Pal, A. Ashok, and A. Ajayan, “Password reuse behavior: How massive online data breaches impacts personal data in web”, in *Innovations in Computer Science and Engineering*, Springer, 2016, pp. 199–210. DOI: 10.1007/978-981-10-0419-3_24.

-
- [52] G. Notoatmodjo and C. Thomborson, “Passwords and perceptions”, in *Proceedings of the Seventh Australasian Conference on Information Security - Volume 98*, ser. AISC '09, Wellington, New Zealand: Australian Computer Society, Inc., 2009, 71–78, ISBN: 9781920682798. [Online]. Available: <https://dl.acm.org/doi/abs/10.5555/1862758.1862770>.
- [53] I. Becker, S. Parkin, and M. A. Sasse, “The rewards and costs of stronger passwords in a university: Linking password lifetime to strength”, in *27th USENIX Security Symposium (USENIX Security 18)*, Baltimore, MD: USENIX Association, Aug. 2018, pp. 239–253, ISBN: 978-1-939133-04-5. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity18/presentation/becker>.
- [54] J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 million passwords”, in *2012 IEEE Symposium on Security and Privacy*, 2012, pp. 538–552. DOI: 10.1109/SP.2012.49.
- [55] I. Ion, R. Reeder, and S. Consolvo, ““...no one can hack my mind”: Comparing expert and non-expert security practices”, in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, Ottawa: USENIX Association, Jul. 2015, pp. 327–346, ISBN: 978-1-931971-249. [Online]. Available: <https://www.usenix.org/conference/soups2015/proceedings/presentation/ion>.
- [56] E. Stobert and R. Biddle, “The password life cycle: User behaviour in managing passwords”, in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, Menlo Park, CA: USENIX Association, Jul. 2014, pp. 243–255, ISBN: 978-1-931971-13-3. [Online]. Available: <https://www.usenix.org/conference/soups2014/proceedings/presentation/stobert>.
- [57] E. Stobert and R. Biddle, “Expert password management”, in *Technology and Practice of Passwords. PASSWORDS 2015. Lecture Notes in Computer Science*,

- vol. 9551, Cham: Springer, 2016, pp. 3–20, ISBN: 978-3-319-29938-9. [Online]. Available: https://doi.org/10.1007/978-3-319-29938-9_1.
- [58] R. Alomari and J. Thorpe, “On password behaviours and attitudes in different populations”, *Journal of Information Security and Applications*, vol. 45, pp. 79–89, 2019, ISSN: 2214-2126. DOI: <https://doi.org/10.1016/j.jisa.2018.12.008>.
- [59] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, D. Margolis, V. Paxson, and E. Bursztein, “Data breaches, phishing, or malware? understanding the risks of stolen credentials”, in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’17, Dallas, Texas, USA: Association for Computing Machinery, 2017, 1421–1434, ISBN: 9781450349468. DOI: [10.1145/3133956.3134067](https://doi.org/10.1145/3133956.3134067).
- [60] P. G. Inglesant and M. A. Sasse, “The true cost of unusable password policies: Password use in the wild”, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI ’10, Atlanta, Georgia, USA: Association for Computing Machinery, 2010, 383–392, ISBN: 9781605589299. DOI: [10.1145/1753326.1753384](https://doi.org/10.1145/1753326.1753384).
- [61] T. Seitz, M. Hartmann, J. Pfab, and S. Souque, “Do differences in password policies prevent password reuse?”, in *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA ’17, Denver, Colorado, USA: Association for Computing Machinery, 2017, 2056–2063, ISBN: 9781450346566. DOI: [10.1145/3027063.3053100](https://doi.org/10.1145/3027063.3053100).
- [62] D. Wang and P. Wang, “The emperor’s new password creation policies”, in *Computer Security – ESORICS 2015. ESORICS 2015. Lecture Notes in Computer Science*, G. Pernul, P. Y A Ryan, and E. Weippl, Eds., vol. 9327, Cham: Springer, 2015, pp. 456–477, ISBN: 978-3-319-24177-7. DOI: https://doi.org/10.1007/978-3-319-24177-7_23.

-
- [63] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, “The tangled web of password reuse.”, in *NDSS*, vol. 14, 2014, pp. 23–26.
- [64] M Yildirim and I. Mackie, “Encouraging users to improve password security and memorability”, *International Journal of Information Security*, vol. 18, no. 6, pp. 741–759, 2019. DOI: <https://doi.org/10.1007/s10207-019-00429-y>.
- [65] R. Dillon, S. Chawla, D. Hristova, B. Göbl, and S. Jovicic, “Password policies vs. usability: When do users go ”bananas”?”, in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 148–153. DOI: [10.1109/TrustCom50675.2020.00032](https://doi.org/10.1109/TrustCom50675.2020.00032).
- [66] K. Hartwig and C. Reuter, “Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations”, *Behaviour & Information Technology*, vol. 0, no. 0, pp. 1–24, 2021. DOI: [10.1080/0144929X.2021.1876167](https://doi.org/10.1080/0144929X.2021.1876167).
- [67] B. Ur, F. Alfieri, M. Aung, L. Bauer, N. Christin, J. Colnago, L. F. Cranor, H. Dixon, P. Emami Naeini, H. Habib, N. Johnson, and W. Melicher, “Design and evaluation of a data-driven password meter”, in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’17, Denver, Colorado, USA: Association for Computing Machinery, 2017, 3775–3786, ISBN: 9781450346559. DOI: [10.1145/3025453.3026050](https://doi.org/10.1145/3025453.3026050).
- [68] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, “How does your password measure up? the effect of strength meters on password creation”, in *21st USENIX Security Symposium (USENIX Security 12)*, Bellevue, WA: USENIX Association, Aug. 2012, pp. 65–80, ISBN: 978-931971-95-9. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur>.

-
- [69] X. D. C. D. Carnavalet and M. Mannan, “A large-scale evaluation of high-impact password strength meters”, *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, May 2015, ISSN: 1094-9224. DOI: 10.1145/2739044.
- [70] C. Scott, D. Wynne, and C. Boonthum-Denecke, “Examining the privacy of login credentials using web-based single sign-on - are we giving up security and privacy for convenience?”, in *2016 Cybersecurity Symposium (CYBERSEC)*, 2016, pp. 74–79. DOI: 10.1109/CYBERSEC.2016.019.
- [71] S.-T. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, and K. Beznosov, “Investigating users’ perspectives of web single sign-on: Conceptual gaps and acceptance model”, *ACM Trans. Internet Technol.*, vol. 13, no. 1, Nov. 2013, ISSN: 1533-5399. DOI: 10.1145/2532639.
- [72] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes”, in *2012 IEEE Symposium on Security and Privacy*, 2012, pp. 553–567. DOI: 10.1109/SP.2012.44.
- [73] E. Griffith. (2021). Two-factor authentication: Who has it and how to set it up, [Online]. Available: <https://uk.pcmag.com/encryption/120042/two-factor-authentication-who-has-it-and-how-to-set-it-up> (visited on Nov. 2021).
- [74] Google. (2020). Google chrome help, [Online]. Available: <https://support.google.com/chrome/answer/95606?co=GENIE.Platform%3DDesktop&hl=en-GB> (visited on May 2020).
- [75] LastPass. (2020). Lastpass website, [Online]. Available: <https://www.lastpass.com> (visited on May 2020).
- [76] KeePass. (2020). KeePass password safe, [Online]. Available: <https://keepass.info/> (visited on May 2020).

-
- [77] P. Arias-Cabarcos, A. Marín, D. Palacios, F. Almenárez, and D. Díaz-Sánchez, “Comparing password management software: Toward usable and secure enterprise authentication”, *IT Professional*, vol. 18, no. 5, pp. 34–40, 2016. DOI: 10.1109/MITP.2016.81.
- [78] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, “Why people (don’t) use password managers effectively”, in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA: USENIX Association, Aug. 2019, pp. 319–338, ISBN: 978-1-939133-05-2. [Online]. Available: <https://www.usenix.org/conference/soups2019/presentation/pearman>.
- [79] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, “Multiple password interference in text passwords and click-based graphical passwords”, in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS ’09, Chicago, Illinois, USA: Association for Computing Machinery, 2009, 500–511, ISBN: 9781605588940. DOI: 10.1145/1653662.1653722.
- [80] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, “Of passwords and people: Measuring the effect of password-composition policies”, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI ’11, Vancouver, BC, Canada: Association for Computing Machinery, 2011, 2595–2604, ISBN: 9781450302289. DOI: 10.1145/1978942.1979321.
- [81] S. G. Lyastani, M. Schilling, S. Fahl, M. Backes, and S. Bugiel, “Better managed than memorized? studying the impact of managers on password strength and reuse”, in *27th USENIX Security Symposium (USENIX Security 18)*, Baltimore, MD: USENIX Association, Aug. 2018, pp. 203–220, ISBN: 978-1-939133-04-5. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity18/presentation/lyastani>.

-
- [82] S. S. Woo, “How do we create a fantabulous password?”, in *Proceedings of The Web Conference 2020*, ser. WWW ’20, Taipei, Taiwan: Association for Computing Machinery, 2020, 1491–1501, ISBN: 9781450370233. DOI: 10.1145/3366423.3380222.
- [83] N. Alkaldi and K. Renaud, “Why do people adopt, or reject, smartphone password managers?”, English, in *EuroUSEC ’16*, 1st European Workshop on Usable Security, EuroUSEC 2016 ; Conference date: 18-07-2016 Through 18-07-2016, Internet Society, 2016, ISBN: 1891562452. [Online]. Available: <https://eurousec.secuso.org/2016/>.
- [84] S. Aurigemma, T. Mattson, and L. Leonard, “So much promise, so little use: What is stopping home end-users from using password manager applications?”, in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.
- [85] R. Ayyagari, J. Lim, and O. Hoxha, “Why do not we use password managers? a study on the intention to use password managers”, *Contemporary Management Research*, vol. 15, no. 4, pp. 227–245, 2019. DOI: <https://doi.org/10.7903/cmr.19394>.
- [86] M. Fagan, Y. Albayram, M. M. H. Khan, and R. Buck, “An investigation into users’ considerations towards using password managers”, *Human-centric Computing and Information Sciences*, vol. 7, no. 1, pp. 1–20, 2017, ISSN: 2192-1962. DOI: 10.1186/s13673-017-0093-6.
- [87] M. Fagan and M. M. H. Khan, “Why do they do what they do?: A study of what motivates users to (not) follow computer security advice”, in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO: USENIX Association, Jun. 2016, pp. 59–75, ISBN: 978-1-931971-31-7. [Online]. Available: <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/fagan>.
- [88] G. A. Fowler. (2019). Password managers have a security flaw. but you should still use one., [Online]. Available: <https://www.washingtonpost.com/>

- technology/2019/02/19/password-managers-have-security-flaw-you-should-still-use-one/ (visited on Apr. 2021).
- [89] M. Carr and S. F. Shahandashti, “Revisiting security vulnerabilities in commercial password managers”, in *ICT Systems Security and Privacy Protection*, M. Hölbl, K. Rannenberg, and T. Welzer, Eds., vol. 580, Cham: Springer, 2020, pp. 265–279, ISBN: 978-3-030-58201-2. DOI: https://doi.org/10.1007/978-3-030-58201-2_18.
- [90] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, “Why older adults (don’t) use password managers”, in *30th USENIX Security Symposium (USENIX Security 21)*, USENIX Association, Aug. 2021, pp. 73–90, ISBN: 978-1-939133-24-3. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity21/presentation/ray>.
- [91] M. Fukumitsu, S. Hasegawa, J.-Y. Iwazaki, M. Sakai, and D. Takahashi, “A proposal of a password manager satisfying security and usability by using the secret sharing and a personal server”, in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016, pp. 661–668. DOI: 10.1109/AINA.2016.45.
- [92] L. Wang, Y. Li, and K. Sun, “Amnesia: A bilateral generative password manager”, in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, 2016, pp. 313–322. DOI: 10.1109/ICDCS.2016.90.
- [93] E. Stobert, T. Safaie, H. Molyneaux, M. Mannan, and A. Youssef, “Bypass: Reconsidering the usability of password managers”, in *Security and Privacy in Communication Networks*, N. Park, K. Sun, S. Foresti, K. Butler, and N. Saxena, Eds., vol. 335, Cham: Springer, 2020, pp. 446–466, ISBN: 978-3-030-63086-7. DOI: https://doi.org/10.1007/978-3-030-63086-7_24.
- [94] N. a. M. Barbosa, J. Hayes, and Y. Wang, “Unipass: Design and evaluation of a smart device-based password manager for visually impaired users”, in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiqui-*

-
- tous Computing*, ser. UbiComp '16, Heidelberg, Germany: Association for Computing Machinery, 2016, 49–60, ISBN: 9781450344616. DOI: 10.1145/2971648.2971722.
- [95] M. Shirvanian, C. R. Price, M. Jubur, N. Saxena, S. Jarecki, and H. Krawczyk, “A hidden-password online password manager”, in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, ser. SAC '21, Virtual Event, Republic of Korea: Association for Computing Machinery, 2021, 1683–1686, ISBN: 9781450381048. DOI: 10.1145/3412841.3442131.
- [96] N. Alkaldi and K. Renaud, “Encouraging password manager adoption by meeting adopter self-determination needs”, in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.
- [97] S. Oesch and S. Ruoti, “That was then, this is now: A security evaluation of password generation, storage, and autofill in browser-based password managers”, in *29th USENIX Security Symposium (USENIX Security 20)*, USENIX Association, Aug. 2020, pp. 2165–2182, ISBN: 978-1-939133-17-5. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity20/presentation/oesch>.
- [98] S. Seiler-Hwang, P. Arias-Cabarcos, A. Marín, F. Almenares, D. Díaz-Sánchez, and C. Becker, ““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*, ser. CCS '19, London, UK: Association for Computing Machinery, 2019, 1937–1953, ISBN: 9781450367479. DOI: 10.1145/3319535.3354192.
- [99] G. M. Beal and J. M. Bohlen, “The diffusion process”, Tech. Rep., 1956.
- [100] F. D. Davis, “Perceived usefulness, perceived ease of use, and user acceptance of information technology”, *MIS Quarterly*, vol. 13, no. 3, pp. 319–340, 1989, ISSN: 02767783. [Online]. Available: <http://www.jstor.org/stable/249008> (visited on Jun. 26, 2022).

-
- [101] M. Golla, M. Wei, J. Hainline, L. Filipe, M. Dürmuth, E. Redmiles, and B. Ur, ““what was that site doing with my facebook password?”: Designing password-reuse notifications”, in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’18, Toronto, Canada: Association for Computing Machinery, 2018, 1549–1566, ISBN: 9781450356930. DOI: 10.1145/3243734.3243767.
- [102] C. Jimenez, P. Lozada, and P. Rosas, “Usability heuristics: A systematic review”, in *2016 IEEE 11th Colombian Computing Conference (CCC)*, 2016, pp. 1–8. DOI: 10.1109/ColumbianCC.2016.7750805.
- [103] E. Wong. (2020). Heuristic evaluation: How to conduct a heuristic evaluation, [Online]. Available: www.interaction-design.org/literature/article/heuristic-evaluation-how-to-conduct-a-heuristic-evaluation (visited on Jul. 2020).
- [104] J. Nielsen, “Enhancing the explanatory power of usability heuristics”, in *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, 1994, pp. 152–158.
- [105] J. Nielsen. (1994). How to conduct a heuristic evaluation, [Online]. Available: <https://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation/> (visited on Nov. 2020).
- [106] J. Nielsen. (1994). Severity ratings for usability problems, [Online]. Available: <https://www.nngroup.com/articles/how-to-rate-the-severity-of-usability-problems/> (visited on Nov. 2020).
- [107] R. Broida. (2019). This is the best free password manager, [Online]. Available: <https://web.archive.org/web/20190916231832/https://www.cnet.com/news/this-is-the-best-free-password-manager/> (visited on Sep. 2019).

-
- [108] R. Broida. (2020). This is the best free password manager, [Online]. Available: <https://www.cnet.com/news/this-is-the-best-free-password-manager/> (visited on Jul. 2020).
- [109] M. Coppock. (2019). The best password managers for 2019, [Online]. Available: <https://web.archive.org/web/20191004232323/https://www.digitaltrends.com/computing/best-password-managers/> (visited on Sep. 2019).
- [110] M. Coppock. (2020). The best password managers for 2020, [Online]. Available: <https://www.digitaltrends.com/computing/best-password-managers> (visited on Jul. 2020).
- [111] N. J. Rubenking. (2019). The best password managers for 2019, [Online]. Available: <https://web.archive.org/web/20190915133410/https://uk.pcmag.com/password-managers/4296/the-best-password-managers> (visited on Sep. 2019).
- [112] N. J. Rubenking. (2020). The best password managers for 2020, [Online]. Available: <https://uk.pcmag.com/password-managers/4296/the-best-password-managers> (visited on Jul. 2020).
- [113] C. Marshall and C. Ellis. (2019). The best free password manager 2019, [Online]. Available: <https://web.archive.org/web/20190915133416/www.techradar.com/uk/news/free-password-manager> (visited on Sep. 2019).
- [114] C. Ellis and B. Turner. (2020). Best password managers in 2020 : Free, paid and business apps for secure password lists, [Online]. Available: <https://www.techradar.com/uk/best/password-manager> (visited on Jul. 2020).
- [115] N. J. Rubenking, B. Moore, and K. Key. (2022). The best password managers for 2022, [Online]. Available: <https://uk.pcmag.com/password-managers/4296/the-best-password-managers> (visited on Jul. 2022).

-
- [116] 1Password. (2022). Find the 1password that’s right for you, [Online]. Available: <https://1password.com/sign-up/> (visited on Jul. 2022).
- [117] Bitwarden. (2022). Choose the plan that fits your needs, [Online]. Available: <https://bitwarden.com/pricing/> (visited on Jul. 2022).
- [118] Zoho. (2022). Free password manager for individuals, [Online]. Available: <https://www.zoho.com/vault/free-password-manager.html> (visited on Jul. 2022).
- [119] RoboForm. (2022). Protect your passwords, [Online]. Available: <https://www.roboform.com/lp?affid=ignuk> (visited on Jul. 2022).
- [120] S. Chiasson, P. C. van Oorschot, and R. Biddle, “A usability study and critique of two password managers”, vol. 15, 2006, pp. 1–16.
- [121] M. B. Miles and A. M. Huberman, *Qualitative data analysis: An expanded source-book*. sage, 1994.
- [122] R. A. Virzi, “Refining the test phase of usability evaluation: How many subjects is enough?”, *Human Factors*, vol. 34, no. 4, pp. 457–468, 1992. DOI: 10.1177/001872089203400407.
- [123] L. Faulkner, “Beyond the five-user assumption: Benefits of increased sample sizes in usability testing”, *Behavior Research Methods, Instruments, & Computers*, vol. 35, no. 3, pp. 379–383, 2003. DOI: <https://doi.org/10.3758/BF03195514>.
- [124] J. Brooke, “Sus: A retrospective”, *Journal of usability studies*, vol. 8, no. 2, pp. 29–40, 2013.
- [125] J. Brooke, “Sus-a quick and dirty usability scale”, *Usability evaluation in industry*, vol. 189, no. 194, pp. 4–7, 1996.
- [126] F. Alodhyani, G. Theodorakopoulos, and P. Reinecke, “Password managers—it’s all about trust and transparency”, *Future Internet*, vol. 12, no. 11, 2020, ISSN: 1999-5903. [Online]. Available: <https://www.mdpi.com/1999-5903/12/11/189>.

-
- [127] JMIR-Publications. (2020). How should p values be reported?, [Online]. Available: <https://support.jmir.org/hc/en-us/articles/360000002012-How-should-P-values-be-reported-> (visited on Oct. 2020).
- [128] Hamilton. (2018). Spss instructions, [Online]. Available: https://academics.hamilton.edu/documents/SPSS_instruction_packet_F18.pdf (visited on Jan. 2021).
- [129] M. Hachman. (2018). Google chrome’s new password manager makes securing chrome even more important, [Online]. Available: <https://www.pcworld.com/article/3303596/google-chrome-new-password-manager.html> (visited on Jul. 2020).
- [130] R. Sinha and K. Swearingen, “The role of transparency in recommender systems”, in *CHI ’02 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA ’02, Minneapolis, Minnesota, USA: Association for Computing Machinery, 2002, 830–831, ISBN: 1581134541. DOI: 10.1145/506443.506619.
- [131] J. Angulo, S. Fischer-Hübner, T. Pulls, and E. Wästlund, “Usable transparency with the data track: A tool for visualizing data disclosures”, in *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA ’15, Seoul, Republic of Korea: Association for Computing Machinery, 2015, 1803–1808, ISBN: 9781450331463. DOI: 10.1145/2702613.2732701.
- [132] C. Sugatan and F. Schaub, “Interactive stories for security education: A case study on password managers”,
- [133] J. Vitale, M. Tonkin, S. Herse, S. Ojha, J. Clark, M.-A. Williams, X. Wang, and W. Judge, “Be more transparent and users will like you: A robot privacy and user experience design experiment”, in *Proceedings of the 2018 ACM/IEEE International Conference on Human-Robot Interaction*, ser. HRI ’18, Chicago, IL, USA: Association for Computing Machinery, 2018, 379–387, ISBN: 9781450349536. DOI: 10.1145/3171221.3171269.

- [134] J. L. Herlocker, J. A. Konstan, and J. Riedl, “Explaining collaborative filtering recommendations”, in *Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work*, ser. CSCW '00, Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 2000, 241–250, ISBN: 1581132220. DOI: 10.1145/358916.358995.
- [135] A. Bangor, P. T. Kortum, and J. T. Miller, “An empirical evaluation of the system usability scale”, *International Journal of Human–Computer Interaction*, vol. 24, no. 6, pp. 574–594, 2008. DOI: 10.1080/10447310802205776.

Appendix A

Appendix

A.1 Chapter 4 (Questions for User Study)

- Take participants' information.
- Which of the following indicates how much you know about password managers?
(* I do not know anything about it, * I know a little, * I know and use it to save my passwords).
- Do you save your passwords in a web browser such as Chrome and Firefox?

Please indicate to what extent you agree or disagree with each of the following statements, on a scale of five: Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), Strongly Disagree (1).

- I find it easy to create an account in a password manager.
- I find it easy to use a password manager.
- It is difficult to install the browser extension of a password manager.
- It is easy to store my online passwords in a password manager.
- I find it hard to change my online passwords in a password manager.
- I find it easy to access my online passwords that are stored in a password manager.

- It is easy to use a password manager on multiple devices.
- It is hard to reset the master password.
- It is easy to find and use random password generator.
- I find it difficult to recover my account if I forget my master password.
- I think I would need help/support to be able to use a password manager.
- Comment:
- How would you describe your overall experience with a password manager? (5) Very satisfied, (4) Satisfied, (3) Neither satisfied nor dissatisfied, (2) Dissatisfied, (1) Very Dissatisfied.
- How satisfied are you with the language used? (5) Very satisfied, (4) Satisfied, (3) Neither satisfied nor dissatisfied, (2) Dissatisfied, (1) Very Dissatisfied.
- What are your thoughts on the design and layout? (5) Excellent, (4) Good, (3) Average, (2) Fair, (1) Poor.
- What did you like the most about using a password manager?
- What did you like the least?
- If you were looking for a random password generator, where would you expect to find it?
- What would you do if password manager fails and you cannot access your passwords?
- How would you save your master password?
- Why are you using a password manager ?
- What platform do you use a password manager on? (iOS, Android, Mac OS, Windows, Linux, Other)

- Did you check the password strength when you created the master password? (Yes, No), Comment:
- Did you check the password strength when you stored Twitter password? (Yes, No), Comment:
- Do you know what will happen if the master password is compromised/stolen? (Yes, No), Comment:
- Would you add an emergency contact to recover your account? (Yes, No), Comment:
- Do you know where a password manager stores your online passwords? (Yes, No), Comment:
- Do you understand how a password manager processes your online passwords? (Yes, No), Comment:
- Would you trust the browser extension of a password manager to fill in your passwords? (Yes, No), Comment:
- Would you trust the vendor of a password manager to store all your online passwords? (Yes, No), Comment:
- Would you trust a password manager to retrieve your account all the time? (Yes, No), Comment:
- Do you store all your passwords on a password manager? (Yes, No I only store some of my passwords), Comment:
- Would you trust a password manager to delete your password permanently from its database after you deleted it from your vault? (Yes, No), Comment:
- Do you know that a password manager synchronizes your passwords across your devices using its own services? (Yes, No), Comment:

- Would you let a password manager store your bank detail and passport information?
(Yes, No), Comment:
- Would you install a browser extension of a password manager on a shared computer to access your passwords? (Yes, No), Comment:
- If you use any kind of password managers, do you create weak passwords (easy to guess passwords) and reuse a password in multiple accounts? (Yes, No), if yes, what is the reason?
- Have you ever used a random password generator? (Yes, No), Comment:
- Do you know that Google Chrome and Firefox offer a built-in password generator?
(Yes, No), Comment:
- **(Non-users of password manager).**

Is there any other reason that makes you abstain or reluctant to use a password manager?
- **(Users of password manager).**

What are the things you would like to improve in a password manager?

All steps completed by participants for LastPass in the user study

1. Create a new account in password manager using this email, a master password.
2. Please install the browser extension of LastPass on the browser.
3. login using the above email and master password that just created.
4. Now, store a new account “Twitter” in the vault. Use the following example: Twitter, account, password. (Don’t forget to check Advanced settings)
5. Please login again using the browser extension. (What do you see?)
6. Return to your vault and view your current password for twitter.

7. To login to Twitter, type `www.Twitter.com` in URL. (Check LastPass extension).
8. In LastPass, change Twitter password automatically using Auto Change password. (What do you see?).
9. If it does not work, use the random generator to generate a new password, copy and paste the new password in Twitter account/website (What happened in LastPass extension?).
10. Go back and check Twitter password in the vault (What do you see?)
11. Now, please reset your master password. (Does the system warn you?)
12. Login using the same email and new Master Password.
13. Please add a phone number ***.
14. Can you please check account settings, untick “Allow reverting LastPass master password changes”?
15. Can you please add a new item “Driver licence” into the menu?
16. Can you please enable the multifactor authentication in LastPass?
17. Can you please add this device to the trusted devices in LastPass?
18. Can you please add this URL `www.facebook.com` to a Never URLs page?
19. Can you add an emergency access to your account? (What do you see?)
20. Let’s assume you forgot your master password; can you please try to recover the account?
21. Can you please use machine number 2 to access your account? (use another computer)
22. Can you please delete twitter account from LastPass vault?
23. Can you please delete LastPass account?

A.2 Chapter 5 (Questions for Online Questionnaire)

- What is your age? (*18-25, *26-35, *36-45, *46-55, *56-65, *66 or older)
- What is your highest level of education? (*Secondary school, *College, *Diploma, *Bachelor for example BSc, *Masters for example MSc, *PhD /Doctorate, *Other)
- Is your educational background related to Computer Science or Information Security? (Yes, No)
- How many online accounts do you have, for example: Banking, Work, University, Social Networks, Entertainment, Emails, Shopping? (*1-5, *6-10, *11-15, *16-20, *21 or more, *I do not know)
- How many unique online passwords do you have? (*1-5, *6-10, *11-15, *16-20, *21 or more, *I do not know)
- On a scale of 5, how important do you consider the passwords of the following accounts (5) Very important, (4) Important, (3) Neutral, (2) Slightly Important, (1) Not at all important. (* Financial accounts e.g. online banking, * Email accounts e.g. gmail, * Shopping accounts e.g. Amazon Next, * Social Networks e.g. Twitter Facebook, * University/School/Work accounts).
- Do you use any kind of a password manager (for example, Firefox, Chrome, LastPass, Dashlane)? (*Yes I use a Password Manager, *No I do not use a Password Manager)

Questions for users of password managers.

- What kind of a password manager do you use? (*LastPass, *Firefox, *Dashlane, *Google Chrome, *Other)
- What platform do you use a password manager on? (*iOS, *Android, *Mac OS, *Windows, *Linux, *Other)

- Have you ever lost/forgot your Master Password? (*Yes, *No, *Not applicable)
- Do you store all your passwords on a password manager? (*Yes, *No I only store some of my passwords)
- How did you hear about a password manager? (*Advertisement, *Social Media, *Family/Friend, *IT Magazine/Article, *Other).
- Why are you using a password manager?
- Do you use a random password generator to generate a unique password for each account? (*Yes, *I only use a random generator for specific accounts, *No).
- If you answered “NO”, what is the reason that applies to you? (*I do not know how to use a random password generator, *I do not know that a password manager offers a built-in random generator, *Other:).

Please indicate to what extent you agree or disagree with each of the following statements, according to the five-point scale Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), Strongly Disagree (1), or Not Applicable (N/A).

Usability of password managers.

- I find it easy to create an account in a password manager.
- I find it easy to use a password manager.
- It is difficult to install the browser extension of a password manager.
- It is easy to store my online passwords in a password manager.
- I find it hard to change my online passwords in a password manager.
- I find it easy to access my online passwords that are stored in a password manager.
- It is easy to use a password manager on multiple devices.

- It is hard to reset the master password.
- I find it difficult to recover my account if I forget my master password.
- I think I would need help/support to be able to use a password manager.

Trusting and understanding password managers.

- I know where my online passwords have been stored in a password manager.
- I fully understand how a password manager processes my online passwords.
- I feel confident to use the browser extension of a password manager to fill in my passwords.
- I trust the vendor of a password manager to store all my online passwords including my sensitive passwords.
- I worry about losing all my passwords that are stored in a password manager.
- I am aware that a password manager will synchronize my passwords across my devices using the vendor's services.
- I trust a password manager to delete my password permanently from its database after I delete it from my vault/browser.
- I fear that a password manager will fail to work or retrieve my passwords, so I store my passwords in a secondary place.
- I fear that all my passwords in a password manager will be exposed if my master password is compromised/stolen.
- I write my master password down and store it in a safe place.
- I have opened my password manager account on a shared computer.
- I would let password manager store my bank details and passport information.

- If you have any comment about password managers, please add it here:

For people who do not use password managers. You stated that you do not use a password manager. Please choose from the list the reasons that apply to you (at least one).

- I find it difficult to use a password manager.
- It is hard to update my passwords in a password manager.
- It is difficult to recover my account if I forget my master password.
- I do not trust the browser extension of a password manager to fill in my passwords.
- I do not trust the 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.
- I do not want to use a password manager because my passwords will be synchronized to my other devices using the 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.
- 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.
- If a password manager fails to work, I will not be able to retrieve my online passwords.
- Other:

A.3 Chapter 6 (Questions for Improving Transparency in Password Managers)

- What is your gender? (*Male, *Female, *Prefer not to say)
- What is your age? (*18-25, *26-35, *36-45, *46-55, *56-65, *66 or older)
- What is your highest level of education? (*Secondary school, *College, *Diploma, *Bachelor's degree, for example BSc, *Master's degree, for example MSc, *PhD /Doctorate, *Other)
- Is your educational background related to Computer Science or Information Security? (Yes, No)
- How many online accounts do you have, for example: Banking, Work, University, Social Networks, Entertainment, Email, Shopping? (*1-5, *6-10, *11-15, *16-20, *21 or more, *I do not know)
- How many unique online passwords do you have? (*1-5, *6-10, *11-15, *16-20, *21 or more, *I do not know)
- What type of device are you using for this study? (*Laptop/Desktop (Windows OS), *Laptop/Desktop (Linux OS), *Laptop/Desktop (Mac OS), *Smartphone (iOS), *Smartphone (Android), *Tablet (iOS), *Tablet (Android), *Other:)

Questions about trust and understanding of non-transparent and transparent password managers. Please indicate to what extent you agree or disagree with each of the following statements, according to the five-point scale: (1) Strongly Disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly Agree.

- I know where my online passwords are stored in non-transparent password manager.

-
- I fully understand how my passwords are processed in non-transparent password manager.
 - I understand how non-transparent password manager works.
 - I understand how non-transparent password manager generates the encryption key.
 - I understand the benefit of a random password generator in non-transparent password manager.
 - I trust non-transparent password manager to store all my online passwords.
 - I trust non-transparent password manager to delete my password from its database permanently after I have deleted it from my account.
 - I trust non-transparent password manager to generate a strong key to encrypt my password.
 - I feel that I have control of my passwords when I store them in non-transparent password manager.
 - Password is stored securely in non-transparent password manager.
 - I trust non-transparent password manager for not synchronizing my passwords over different devices (e.g. computers, smartphones) without my permission.
 - I know where my online passwords are stored in transparent password manager.
 - I fully understand how my passwords are processed in transparent password manager.
 - I understand how transparent password manager works.
 - I understand how transparent password manager generates the encryption key.
 - I understand the benefit of a random password generator in transparent password manager.

- I trust transparent password manager to store all my online passwords.
- I trust transparent password manager to delete my password from its database permanently after I have deleted it from my account.
- I trust transparent password manager to generate a strong key to encrypt my password.
- I feel that I have control of my passwords when I store them in transparent password manager.
- Password is stored securely in transparent password manager.
- I trust transparent password manager for not synchronizing my passwords over different devices (e.g. computers, smartphones) without my permission.
- Do you use a password manager (for example, Firefox, Chrome, LastPass, Dashlane)? (*Yes I use a password manager, *No I do not use a password manager).

For non-users of password managers.

- Would you adopt a password manager if it is the same as transparent password manager? (*Yes I would adopt it, *No I would not adopt it.)
- If you answered (Yes), what is the reason that would make you use transparent password manager? (*It is trustworthy, *I understand how it works, *It is easy to use, *It is secure)
- If you answered (No), what is the reason for your answer?

For users of password managers.

- What password manager do you use? (*Chrome, *LastPass, *Dashlane, *1Password, *Other:)

This section is only about Transparent Password Manager (Usability). Please indicate to what extent you agree or disagree with each of the following statements, according to the five-point scale: (1) Strongly Disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly Agree. The System Usability Scale (SUS) questions.

- I think that I would like to use this system frequently.
- I found the system unnecessarily complex.
- I thought the system was easy to use.
- I think that I would need the support of a technical person to be able to use this system.
- I found the various functions in this system were well integrated.
- I thought there was too much inconsistency in this system.
- I would imagine that most people would learn to use this system very quickly.
- I found the system very cumbersome to use.
- I felt very confident using the system.
- I needed to learn a lot of things before I could get going with this system.
- I am satisfied with the language used in transparent password manager. (1) Very Dissatisfied, (2) Dissatisfied, (3) Neither satisfied nor dissatisfied, (4) Satisfied, (5) Very Satisfied.
- What are your thoughts on the design and layout of transparent password manager? (1) Poor, (2) Fair, (3) Average, (4) Good, (5) Excellent.
- What do you like the most in transparent password manager?
- What do you dislike the most in transparent password manager?
- Are there any comments you would like to add regarding this study?

A.4 Chapter 7 (Questions for Improving Transparency in Password Managers “extended study”)

- What is your gender? (*Male, *Female, *Prefer not to say)
- What is your age? (*18-25, *26-35, *36-45, *46-55, *56-65, *66 or older, *Prefer not to say)
- What is your highest level of education? (*Secondary school, *College, *Diploma, *Bachelor’s degree, for example BSc, *Master’s degree, for example MSc, *PhD /Doctorate, *Other)
- In which sequence did you use the two programs? (*First Program A, and then Program B) (*First Program B, and then Program A)
- Is your educational background related to Computer Science or Information Security? (Yes, No)
- How many online accounts do you have, for example: Banking, Work, University, Social Networks, Entertainment, Email, Shopping? (*1-5, *6-10, *11-15, *16-20, *21 or more, *I do not know)
- How many unique online passwords do you have? (*1-5, *6-10, *11-15, *16-20, *21 or more, *I do not know)
- What type of device are you using for this study? (*Laptop/Desktop (Windows OS), *Laptop/Desktop (Linux OS), *Laptop/Desktop (Mac OS), *Smartphone (iOS), *Smartphone (Android), *Tablet (iOS), *Tablet (Android), *Other:)
- Do you use a password manager (for example, Firefox, Chrome, LastPass, Dashlane)? (*Yes I use a password manager, *No I do not use a password manager).

Questions about trust and understanding of Program A and B. Please indicate to what extent you agree or disagree with each of the following statements, according

to the five-point scale: (1) Strongly Disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly Agree

- I know where my online passwords are stored in program A.
- I fully understand how my passwords are processed in program A.
- I understand how program A works.
- I understand how program A generates the encryption key.
- I understand the benefit of a random password generator in program A.
- Paris is the capital of Spain.
- I trust program A to store all my online passwords.
- I trust program A to delete my password from its database permanently after I have deleted it from my account.
- I trust program A to generate a strong key to encrypt my password.
- I feel that I have control of my passwords when I store them in program A.
- Password is stored securely in program A.
- I trust program A to not synchronize my passwords over different devices (e.g. computers, smartphones) without my permission.
- I know where my online passwords are stored in program B.
- I fully understand how my passwords are processed in program B.
- I understand how program B works.
- I understand how program B generates the encryption key.
- I understand the benefit of a random password generator in program B.

- Madrid is the capital of France.
- I trust program B to store all my online passwords.
- I trust program B to delete my password from its database permanently after I have deleted it from my account.
- I trust program B to generate a strong key to encrypt my password.
- I feel that I have control of my passwords when I store them in program B.
- Password is stored securely in program B.
- I trust program B to not synchronize my passwords over different devices (e.g. computers, smartphones) without my permission.

This section is about program A and program B.

- Which program do you prefer? (*Program A, *Program B)

For participants who preferred program A.

- Why do you prefer program A?.

For participants who preferred program B. From your point of view, what are the advantages of program B. On a scale of 1 to 4, how important are the following factors for choosing program B, (1) Not important at all, (2) Slightly important, (3) Important, (4) Very important.

- I can choose a place to store passwords.
- It shows me the location of stored passwords.
- I can generate an encryption key to encrypt each password.
- It shows me the encryption key that is used to encrypt passwords.

- I can prevent/allow password synchronization for each password.
- It shows me the stored password in an encrypted form.
- It shows me the date and time when the password was last stored.
- The buttons in program B are coloured and are visible.
- The text boxes that explain features such as the benefit of password generator.

This section is only about Program B (Usability). Please indicate to what extent you agree or disagree with each of the following statements, according to the five-point scale: (1) Strongly Disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly Agree. The System Usability Scale (SUS) questions.

- I think that I would like to use this system frequently.
- I found the system unnecessarily complex.
- I thought the system was easy to use.
- I think that I would need the support of a technical person to be able to use this system.
- I found the various functions in this system were well integrated.
- I thought there was too much inconsistency in this system.
- I would imagine that most people would learn to use this system very quickly.
- I found the system very cumbersome to use.
- I felt very confident using the system.
- I needed to learn a lot of things before I could get going with this system.
- I am satisfied with the language used in program B. (1) Very Dissatisfied, (2) Dissatisfied, (3) Neither satisfied nor dissatisfied, (4) Satisfied, (5) Very Satisfied.

- What are your thoughts on the design and layout of program B? (1) Poor, (2) Fair, (3) Average, (4) Good, (5) Excellent.
- What do you like the most in program B?
- What do you dislike the most in program B?
- Are there any comments you would like to add regarding this study?

A.5 More Comments and Tables for Chapter 4, 5, 6, 7

Table A.1: For the question “How would you save master password?”

Code	Sample of comments (Chapter 4)
Memorize it	<ul style="list-style-type: none"> • Memorize it only. • Memorize it.
Save it somewhere	<ul style="list-style-type: none"> • Save it on my smartphone. • Write it on my phone.

Table A.2: For the question “Install a browser extension on a shared computer?”

Code	Sample of comments (Chapter 4)
Security concern	<ul style="list-style-type: none"> • Because the machine might be compromised. • Someone else might access my account.
Forget to log out	<ul style="list-style-type: none"> • I may forget to log out. • In case if I forget to log out.

Table A.3: For the question “Checked the strength of master password?”

Code	Sample of comments (Chapter 4)
Weak policy	<ul style="list-style-type: none"> • Weak policy. • Not strong enough. • They should use the special characters.
Good indicator	<ul style="list-style-type: none"> • Good indicator to create master password.

Table A.4: For the question “What will happen if master password is compromised?”

Code	Sample of comments (Chapter 4)
Compromised passwords	<ul style="list-style-type: none"> • All password will be accessed by the attacker. • All stored passwords will be compromised. • All passwords will be compromised. Master password is a great idea to have but it has high security threat.

Table A.5: For the question “What did you like the least?”

Code	Sample of answers (Chapter 4)
Lack of flexibility (users)	<ul style="list-style-type: none"> • It kept promoting you to enter master password. • Ask for a verification for a new device.
Design not user friendly (non-users)	<ul style="list-style-type: none"> • Not user friendly. • Design and the language. • It looks complicated.
Complexity and ambiguity (users)	<ul style="list-style-type: none"> • Loads of options and things hidden. • The maze and complicated. • Ambiguity.
Lack of flexibility (non-users)	<ul style="list-style-type: none"> • Keep entering my master password. • The issue of switching devices.
Security concerns (users)	<ul style="list-style-type: none"> • Risk it if there is any hack on all passwords. • Taking all my passwords under one password.

Table A.6: For the question “Where would you expect to find a random generator?”

Code	Sample of comments (Chapter 4)
Account settings	<ul style="list-style-type: none"> • Account setting. • The auto generator and generator should be in the settings or together.
Main page (vault)	<ul style="list-style-type: none"> • Direct link in the main page (vault) • Main page (vault).
Browser extension	<ul style="list-style-type: none"> • Good to have it in the browser extension. • In the top right (in browser extension).
Password dialogue box	<ul style="list-style-type: none"> • In the passwords dialog box. • In the password field next to twitter icon in password box.

Table A.7: For the question “What would you do if password manager fails to work?”

Code	Sample of comments (Chapter 4)
Call help centre	<ul style="list-style-type: none"> • Call help center. • Call the company.
Enter it manually	<ul style="list-style-type: none"> • I enter passwords manually. • Login manually.
Use forget password	<ul style="list-style-type: none"> • Use forget password in the website. • I will reset the password for the current site I use.
Use offline version	<ul style="list-style-type: none"> • Use offline version of the software.
Save it in another place	<ul style="list-style-type: none"> • I will save my passwords somewhere. • Save my passwords in phone.

Table A.8: For the question “Why are you using a password manager?”

Code	Sample of comments (Chapter 4)
Save passwords	<ul style="list-style-type: none"> • To store the passwords. • I cannot remember my passwords, so I save them in a password manager. • In case I forgot my passwords, it will bring it to me.
Easy access	<ul style="list-style-type: none"> • Easy to access my accounts. • To make it easy to access accounts.
Security reason	<ul style="list-style-type: none"> • Secure my passwords.
Manage passwords	<ul style="list-style-type: none"> • To manage my passwords. • If I used it, I would use it to have a strong management of passwords.

Table A.9: For the question “Add emergency contact to recover the account?”

Code	Sample of comments (Chapter 4)
Good feature	<ul style="list-style-type: none"> • The best features in password manager.
Trust issue	<ul style="list-style-type: none"> • It is difficult to find someone to trust.
Should be free	<ul style="list-style-type: none"> • If it is free, I would use emergency for another second personal account.

Table A.10: For the question “Let a password manager store bank and passport details?”

Code	Sample of comments (Chapter 4)
Security concern	<ul style="list-style-type: none"> • Security reason. • Sensitive information.
Trust issue	<ul style="list-style-type: none"> • I would not trust them with this information. • I do not have a high-level of trust in password manager.

Table A.11: For the question “Reuse password in multiple accounts?”

Code	Sample of comments (Chapter 4)
Easy to remember	<ul style="list-style-type: none"> • Easy for me to remember. • Cause I don't want to forget it. • Short memory space. • Laziness and limit number of times attempt login.

Table A.12: Answers sample for not using a password generator (Chapter 5). Frequencies of codes being applied to participants' reasons for not using random generator. The numbers add up to 100%. Participant's answer could have different reasons.

%	Code	Sample of answers (Chapter 5)
19%	Hard and complex to remember	<ul style="list-style-type: none"> • Too complex in case I have to remember the password. • I like to memorize my passwords, and it is hard to memorize generated passwords. • I cannot remember the passwords suggested in case I need to manually enter my password. • Hard to type in when autofill not available. • I don't like auto generated passwords. Harder for me to remember.
7%	Create memorable passwords	<ul style="list-style-type: none"> • I prefer to have a complex password depends on some events in my life. • I need to use a password that I can recall. • I prefer to create my own password that I can remember.

Table A.13: Comparing between non-transparent and transparent managers (Chapter 6). Using a Wilcoxon Signed-Ranks test to find mean ranks (negative and positive).

	Questions	Negative ranks	Positive ranks
1	I know where my online passwords are stored.	25.17	52.82
2	I fully understand how my passwords are processed.	28.11	52.52
3	I understand how it works.	34.41	45.58
4	I understand how it generates the encryption key.	25.78	43.44
5	I understand the benefit of a random password generator.	35.18	39.17
6	I trust it to store all my online passwords.	32.03	47.57
7	I trust it to delete my password from its database permanently after I have deleted it from my account.	24.73	46.84
8	I trust it to generate a strong key to encrypt my password.	33.00	50.84
9	I feel that I have control of my passwords when I store them.	38.87	50.88
10	Password is stored securely.	32.36	38.70
11	I trust it for not synchronizing my passwords over different devices without my permission.	34.43	54.71

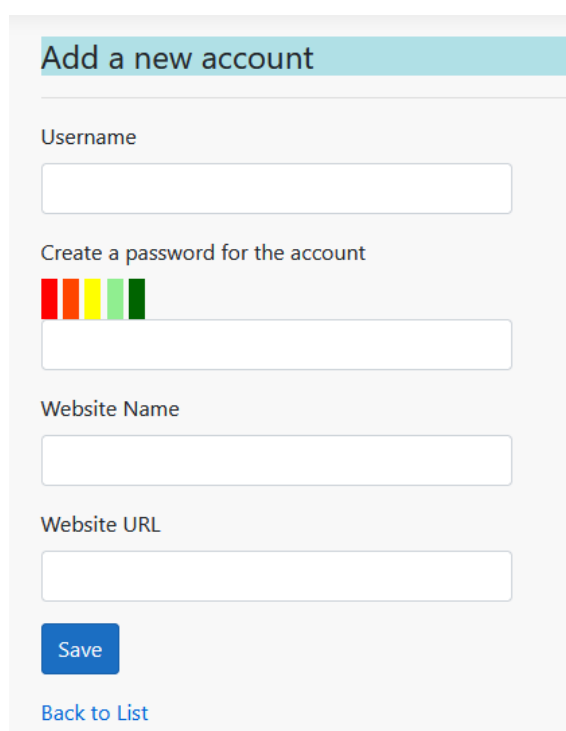
Table A.14: Comparing between program A and program B (Chapter 7). Using a Wilcoxon Signed-Ranks test to find mean ranks (negative and positive).

	Questions	Negative ranks	Positive ranks
1	I know where my online passwords are stored.	17.97	29.35
2	I fully understand how my passwords are processed.	16.25	20.37
3	I understand how it works.	19.12	21.88
4	I understand how it generates the encryption key.	19.14	26.53
5	I understand the benefit of a random password generator.	17.79	22.33
6	I trust it to store all my online passwords.	17.63	25.13
7	I trust it to delete my password from its database permanently after I have deleted it from my account.	11.00	21.32
8	I trust it to generate a strong key to encrypt my password.	8.50	26.98
9	I feel that I have control of my passwords when I store them.	18.70	25.43
10	Password is stored securely.	22.75	27.76
11	I trust it to not synchronize my passwords over different devices without my permission.	15.14	25.55

A.6 More Screenshots for two Programs (Chapter 6 / 7)

This section contains screenshots from the programs (non-transparent/program A, and transparent/program B). Please note that the website and the codes are not publicly available. You can contact the researcher for more information.

Screenshots from non-transparent manager/program A:



The screenshot shows a web form titled "Add a new account" with a light blue header. The form contains the following fields and elements:

- Username:** A text input field.
- Create a password for the account:** A text input field with a password strength indicator above it consisting of five colored bars (red, yellow, green, light green, dark green).
- Website Name:** A text input field.
- Website URL:** A text input field.
- Save:** A blue button.
- Back to List:** A blue link.

Figure A.1: Adding an account in non-transparent/program A, there are only forms for username, password and website name/URL. Password generator buttons are in colour. When saving a new password, the program informs user that the password has been stored.

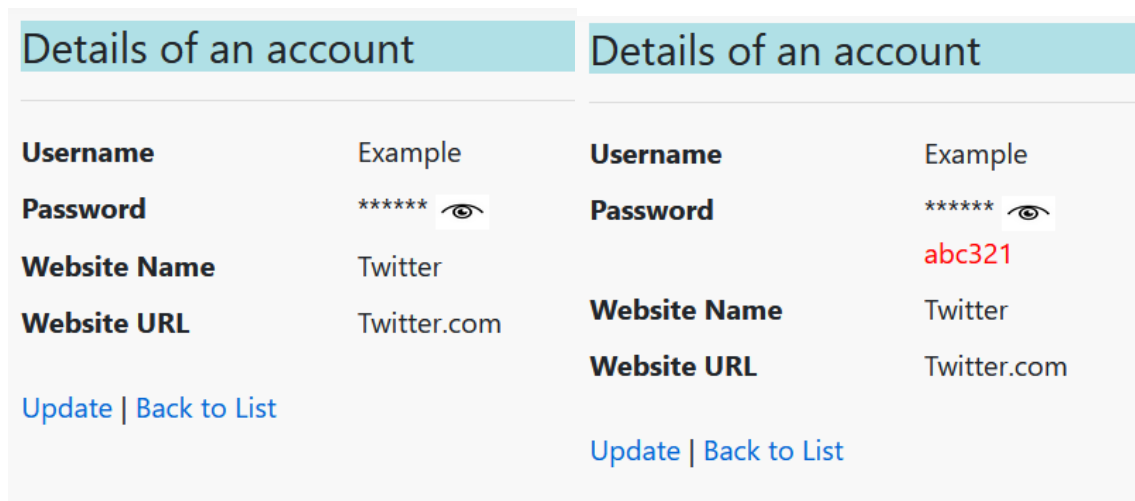


Figure A.2: Details page of program A, it only shows a username, password (asterisk) and website name/URL. The second screenshot shows the password when a user puts the cursor on the eye icon.



Figure A.3: Main page of program A which shows a stored account. The page shows website name/URL, username and password as asterisk. The second screenshot shows the password when a user puts the cursor on the eye icon.

Screenshots from transparent manager/program B:

Add a new account

Username

Website Name

Website URL

Encryption Key ?

Encryption Key ?

Create a password for the account

View the map of locations and then select a place from the list to store the account (simulated)

Do you want to synchronize your password over different devices (computers, smartphones) using password manager service? (simulated)

[Back to List](#)

Figure A.4: Adding an account page in transparent/program B. There is a button to generate an encryption key to encrypt the password, different options to choose from to store each password and view the location on Google maps. A random password can be generated using a random password generator which shows the strength of password in words and colours. Finally, password synchronization can be allowed or prevented.

The figure consists of two side-by-side screenshots of a web form. The left screenshot shows the form with the 'Generate an encryption key' button highlighted in green. A tooltip below it says 'This key will encrypt your password'. The right screenshot shows the form after the button is clicked. The 'Encryption Key ?' field now contains the key '[5pKQKMy\$QyieMogTzy4K2X0\$FXUxmQ7]'. The password strength indicator shows 'Very Strong' selected.

Figure A.5: Adding an account page in transparent/program B. The screenshot on the left shows a button that generates an encryption key when a user puts the cursor on. The screenshot on the right shows the generated key (the button disappears once it is clicked).

The figure shows a single screenshot of the web form. The password field now contains the random password 'zETSQto5vCHI'. The password strength indicator shows 'Very Strong' selected.

Figure A.6: Adding an account page in transparent/program B. The random password generator generates different types of passwords such as very weak and strong.

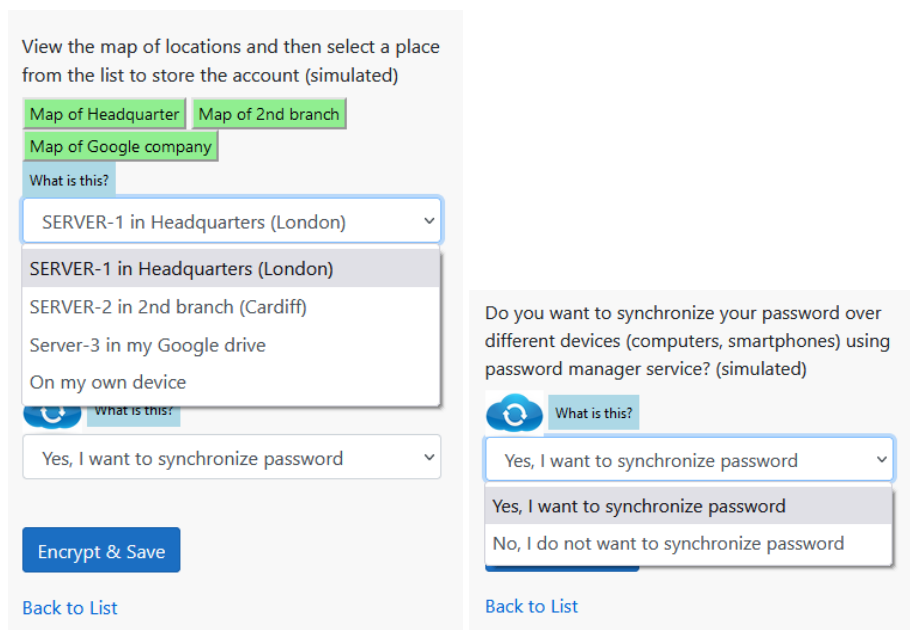


Figure A.7: Adding an account page in transparent/program B. The program offers different storage locations to store passwords, e.g., Headquarters. It also offers an option where passwords can be synchronized across devices or prevented (all simulated).

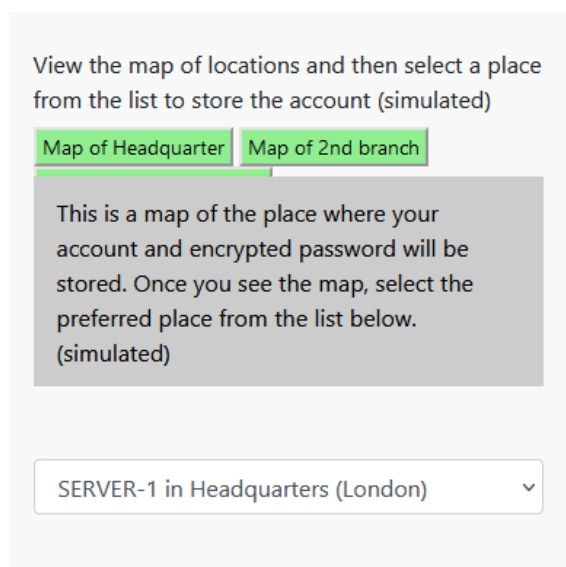


Figure A.8: Adding an account page in transparent/program B. When a user puts the cursor on the text box, it shows an explanation about the storage location.

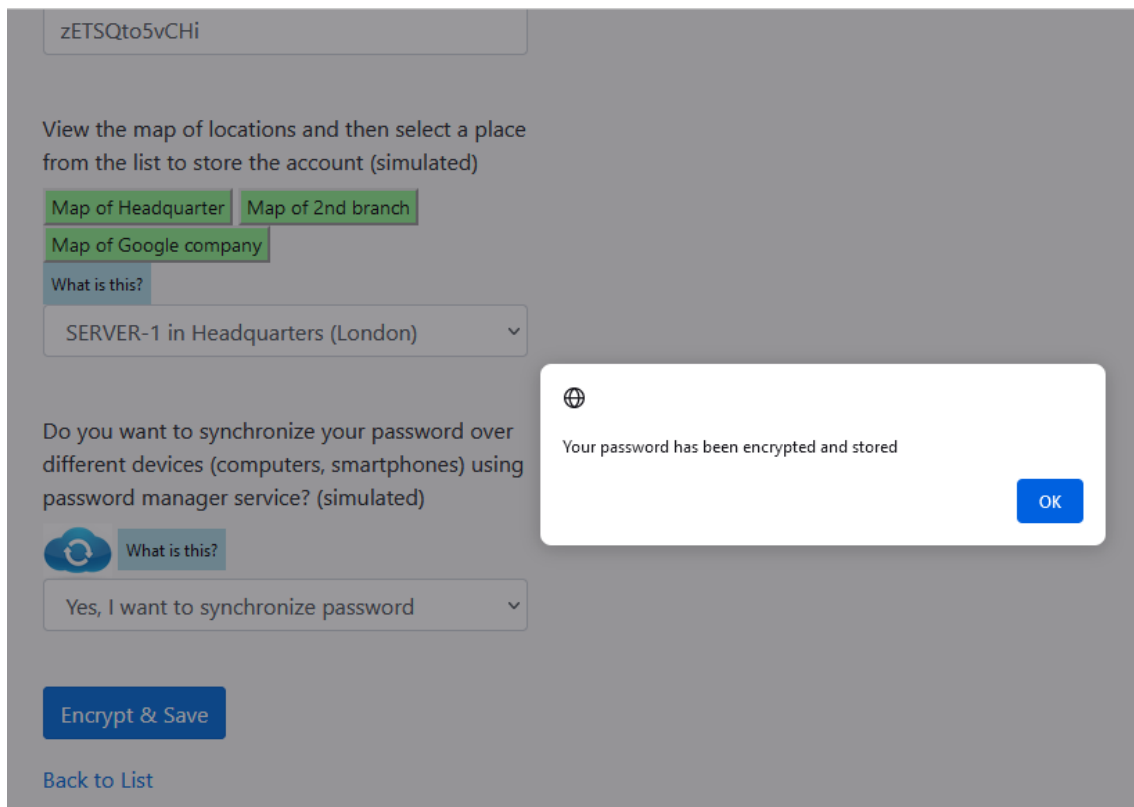


Figure A.9: Adding an account page in transparent/program B. When the button “Encrypt and Save” is clicked, the new password will be encrypted and saved. The link (URL) of the program is hidden in the screenshot.

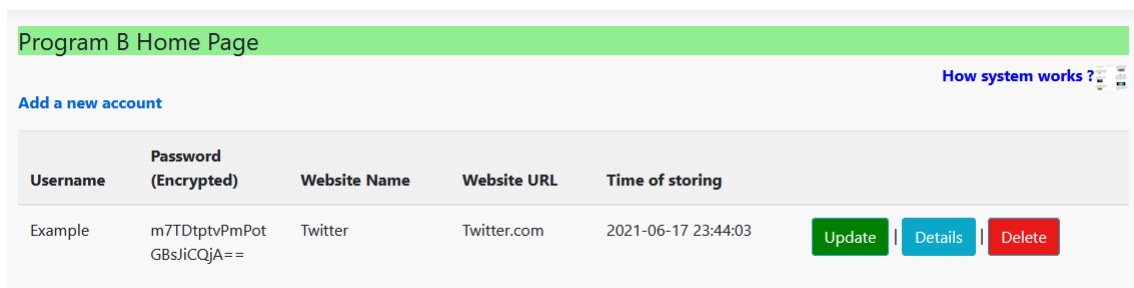


Figure A.10: Main page of transparent/program B which shows a stored account. The page shows website name/URL, username, encrypted password and time of storing it.

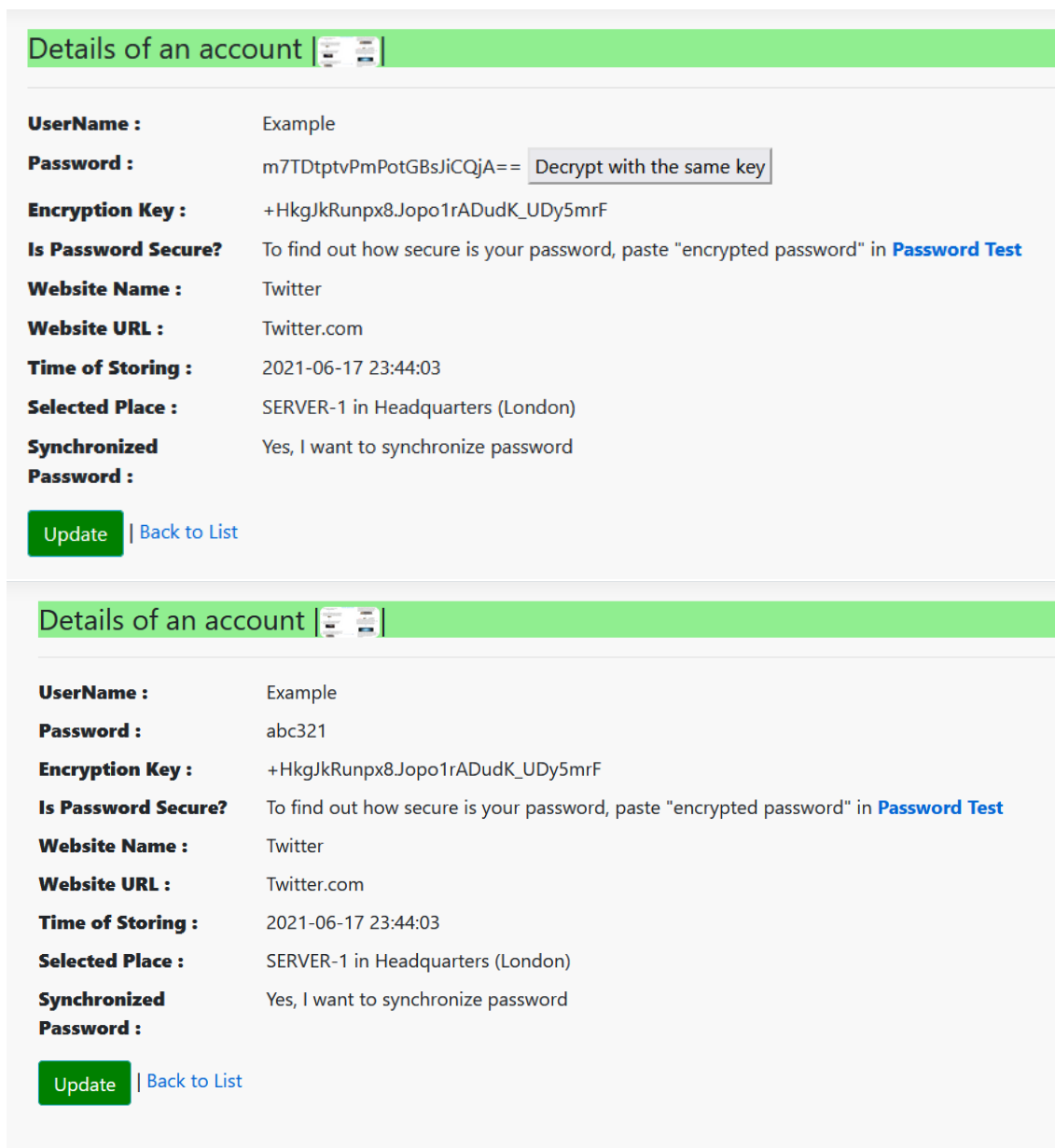


Figure A.11: Details page of transparent/program B. The page shows the username, encrypted password, encryption key, time of storing, location and synchronization. The password can be decrypted by clicking on the button (second screenshot). Also, there is an external link to check the strength of stored password.