UNDERSTANDING MENTAL MODELS OF PASSWORD MANAGERS

by

Svetlana Dobrynina

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF ARTS

Human Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
August, 2023

Abstract

Password managers are tools that create and store passwords, and are widely viewed as a secure and convenient password management strategy. However, these tools are under-adopted. This research investigates users' mental models of password managers and aims to understand their motivations for adopting these tools. We conducted an online survey with 197 participants and an interview study with 21 participants, who were divided into three groups: users of dedicated password managers, users of browser-based managers, and non-users. Participants' password management approaches ranged from relying on default options, such as saving passwords in web browsers, to deliberate decisions to break with previous habits, such as adopting dedicated programs. Our thematic analysis showed that users' adoption of password managers is influenced by their understanding of online security. We suggest that increasing the transparency of password manager properties to users and leveraging their trust in smartphones could induce effective adoption of password managers.

Acknowledgements

I am very grateful to my supervisor Elizabeth Stobert for the opportunity to work with her and for inspiring me to study this fascinating topic of online security. Her professional guidance, almost daily support, and encouragement throughout the research process helped me to develop my academic skills and complete this project.

I also want to express my gratitude to Sonia Chiasson for her high-level expertise and thoughtful insights, which helped me broaden my understanding of the discipline.

I am honored to have had the privilege of working under the supervision of the two great professors who have enriched my academic experience. Thank you both for your time and strong support!

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

Passwords are still considered the most common online authentication method [6,16] even though the goal of finding another seamless yet secure authentication process has been a longstanding concern for over decades [6]. Due to the growing number of accounts and a limited number of items the human brain is able to remember, people tend to find different coping strategies to reduce memory overload and find convenient ways to manage their passwords [6,23,24,39,44,46]. Some strategies (such as password reuse) make user accounts vulnerable to guessing attacks [16,36,44]. Security experts suggest the adoption of password managers, specialized tools for secure and convenient management of online accounts [7,12,42]. Experts distinguish two types of password managers: dedicated and built-in. This research aims to understand online users' perception of built-in browser and dedicated password managers (which have lower rates of adoption), explore their motivation and decision-making processes for adoption of these tools, and define users' mental models of browser-based and dedicated programs.

Adoption of password managers is driven by a set of interrelated factors which encourage password manager use, such as awareness of the tool, perception of enhanced security, anticipated ease of learning and use, and positive experience of other people [2,12,23]. Concerns over trust and transparency may, conversely, hinder adoption: people feel uncomfortable not being aware of how a tool stores user passwords and also have a fear of losing control of their accounts by saving all passwords in one place [3,4,12,23,32]. Time and the perceived excessive amount of effort required to find, install, and learn the tool also limits users' interest in adopting password managers [1,4,12].

Existing research indicates differences in password management habits and motivations to adopt password managers among users and non-users. But there is little research on the habits and perceptions between those who have adopted different types of password managers — browser-based and dedicated programs. For example, little is known about how users of dedicated password managers choose these tools or what is the nature of their decision-making process to start using this type of manager compared to users of browser-based managers. There is also little research into the security considerations of the two types of password manager users, or those of non-users.

1.2 Research questions

In general, we are interested in mental models of password managers for different categories of users. We conducted two studies: an online survey with 197 participants and an interview study with 21 participants. We created three research questions, each investigating a different aspect of how people use and understand password managers:

RQ1 What are the password management habits in three groups of Internet users:

- users of dedicated password managers
- users of browser-based password managers
- non-users

RQ2 What are perceptions of browser-based and dedicated password managers in three groups?

RQ3 What are users' decision-making processes for using (or not using) password managers in all three groups?

1.3 Contributions

In this thesis, we made a number of contributions. Our first study of 197 users provided empirical data showing password management strategies for three groups: users of dedicated password managers, users of browser-based managers, and non-users.

We conducted a thematic analysis of 21 semi-structured interviews with password manager users and non-users. Our thematic analysis identified underlying phenomenon for a variety of password management strategies and differences in adoption of password managers among users. We suggest that understanding of online security defines users' approaches to managing their accounts. We found that users in the dedicated password manager group had a more sophisticated mental model of online security and most of them practiced secure password management habits, compared to other user groups who mostly had simple and reused passwords.

Based on both studies, we describe the mental models of password managers in three groups of participants. Users of dedicated password managers trusted dedicated programs, considered them as a convenient solution for secure password management, knew how these tools work, and used browser-based managers only as a backup for noncritical accounts. The mental models for browser-based manager users were based on the assumption that browser-based managers are simple and convenient tools for storing passwords, and dedicated programs are unnecessary tools that can create usability issues. Non-users generally were distrusting of both types of tools, considering them insecure because of their connection to the Internet.

Based on our findings, we made recommendations for encouraging the adoption of password managers. We suggest leveraging trust in smartphones, where smartphones are considered the default devices for storing passwords. We recommend training and education with the active role of large trusted institutions in promoting secure online habits and adoption of password managers. We also suggest improvements to the tools' features to make their benefits more transparent to users and addressing some usability issues.

1.4 Thesis Outline

The remainder of this thesis is organized as follows:

- **Chapter 2** provides an overview of related research examining the password authentication paradigm, the security and usability of password managers as specialized tools for managing passwords, factors influencing the adoption of these tools, and differences in the perception of password managers by different types of users.

- **Chapter 3** reports the methodology and results of an online survey that examined the password management habits of 197 participants.
- **Chapter 4** presents the methodology and results of an interview study in which we interviewed 21 participants divided into three groups: dedicated password manager users, browser-based manager users, and non-users. We explored in detail our participants' motivation and decision-making processes about their password management strategies.
- **Chapter 5** presents our interpretation of the mental models of password managers in each of the three groups, based on our two studies.
- **Chapter 6** discusses the implications of our findings for encouraging the use of password managers and our recommendations. It also discusses the limitations of the studies and future work.
- **Chapter 7** summarizes our work and offers our concluding remarks.

Chapter 2

Background

The term “mental model” is widely used in the field of HCI; it examines people’s perception of a computer system (i.e., how users perceive its purposes, functions, and states) and explains why and how people interact with the system [45]. Led by their mental models of online security, people make various security decisions to align their attitudes with their actual online behavior. Typically, the chosen online behavior is the result of a compromise between security and convenience [43]. As Dourish et al. showed, on the one hand, the decisions are made depending on the answer on the following fundamental question about security: “is this computer system secure enough for what I want to do now?” [10, p. 399]. On the other hand, security is often perceived as an obstacle to normal online routine [10], as people are required to be authorized by the system to receive access to their personal environment [6].

Passwords are the most common authentication method which gives access to users’ online accounts, but they are also perceived as a barrier since remembering and managing them puts an additional burden on users [13, 39, 46]. This prompts people to find various coping strategies to overcome this inconvenience [16, 24, 44, 49]. Security experts report the existence of various weak coping strategies among online users (such as password reuse, creating easy-to-guess passwords, or unprotected password storing) [6, 24, 39, 46, 49], while recommending other strategies that make password management secure. One important strategy is adoption of password managers, dedicated tools for securely creating, storing, and using passwords [12, 20, 42].

The subsequent discussion will provide further insights into existing approaches for online authentication, the password concept as the most ubiquitous authentication method, and the common strategies people use to manage their passwords. This will be followed by discussion of recent studies on password managers and factors that influence password managers’ adoption. We will also explore the topic of mental models in online security and discuss how incorrect or incomplete mental models can lead to weak online behaviour.

2.1 Password authentication paradigm

The need for online authentication, with its primary purpose to protect user accounts and sensitive data from theft, has been a longstanding concern for over four decades. Since then, experts have been working on solving the issue of seamless yet secure authorization process [6]. Despite intensive research into alternatives, passwords are still considered the most ubiquitous method for gaining authorized access to an account [6,16]. Since proposed security solutions for online authentication traditionally include security and usability trade-offs [16], the academic community has long been trying to find alternatives to password authentication that are more reliable, require less time and effort from users, but at the same time provide a high level of security [6,16,40].

2.1.1 Password alternatives and ubiquity of passwords

Back in 2015, Bonneau et al. [6] analyzed various password alternatives, including graphical passwords, biometric passwords, security tokens, password managers, and single sign-on protocols. While some of these replacement schemes provide more security, usability or deployability benefits, passwords are still a universal way to protect user data from attacks and leaks.

In particular, *biometric authentication* (such as face, iris, voice, or fingerprint recognition) has high rate of acceptance among users due to its convenience [6] and improved security due to uniqueness of each user's biometric information [33]. However, the system is still vulnerable to threats, in particular, it can be an object of replay attacks, accompanied by a serious privacy compromise: attackers may steal or tamper the biometric information during storage or transmission and replay it in the next authentication session. Attackers can also use a fake finger or voice record to compromise user account [33]. Moreover, biometric authentication requires additional hardware for wide deployment [6].

Security keys (or security tokens), such as YubiKey, are more user-friendly and provide more data security (as they stop users from re-using passwords, and provide some protection from phishing and man-in-the middle attacks) [19]. At the same time, there is an issue of trust in token manufacturers, who have to prove that they develop and implement secure software and hardware without any intentional and unintentional vulnerabilities and that the tokens are not subject to any manipulation during distribution [34]. Hardware tokens have higher cost per user [19] and, as a physical authenticator, can be simply lost or stolen.

Graphical passwords are promising schemes in terms of memorability but have some implementation limitations on different screen sizes and require careful implementation to increase security (e.g., by implementing more click-points and prompting users against points' clustering for better memorization) [41]. Graphical schemes also have longer login times in general and do not offer protection against shoulder surfing [38].

In contrast, passwords require no hardware or any special equipment [5], give access to user accounts from everywhere [16], and work in diverse environments, technology platforms, cultures, and applications [6]. Passwords offer the cheapest way for ubiquitous implementation, and have clear backward compatibility with no migration costs [6]. From the user's perspective, passwords surpass other methods because they are the most familiar way to authorize (it is hard "to overcome change-resisting inertia", [6, p. 83]) and require little adoption effort from users.

2.1.2 Security and usability of passwords

Despite being ubiquitous, password authorization still poses some challenges for usability (when a user needs to memorize all their passwords or find strategies for reliable password storing) and for security [5]. An average person has 70-80 passwords for access to their accounts [48] and some studies indicate even up to 130 accounts per user [9]. User passwords are desirable targets for theft by cybercriminals as they may open the door to other accounts of the same user that allows hackers access to additional personal data. Unauthorized access to a user's password can be obtained through offline or online guessing attacks, social engineering (e.g., phishing attacks) [5,13], keystroke logging harvests, eavesdropping [16], or improper password management by website administrators (e.g., if password files are not salted and hashed or if a password reset procedure for possibly compromised user accounts is not set up) [6,13].

Although almost no user account is capable of withstanding brute-force offline attacks, it is possible to minimize risks from online attacks by having a strong, or guess-resistant password to withstand 10^6 guesses [13]. To help users manage passwords appropriately and protect their accounts against brute-force attacks, information security professionals should regularly update password policies according to the most recent standards. The National Institute of Standards and Technology (NIST) is the most prominent institution that develops cybersecurity guidelines [25]. At present, the latest NIST recommendations (as of 2017, with updates from 2020) suggest that passwords must not consist of dictionary phrases, sequential characters and digits or context-specific words (such as the name of the service), compromised passwords from previous breach cases, and be at least 8 characters long.

2.1.3 User strategies for password management

Since the human brain can memorize a limited number of items, people tend to find different coping strategies to reduce memory overload and find convenient ways to create and manage their passwords. The results of various password studies suggest that the main coping strategies are:

(a) password reuse across multiple web sites or modification of the existing passwords [6,23,39,46];

(b) creating passwords that are easy to remember: i.e., the use of predictable sequences of digits or characters, dictionary words or substitution of letters with digits and special characters in dictionary words [39,46], the use of personal information or the name of the service [44];

(c) keeping old passwords (i.e., no habit of password change) in the event of a password leak or after using a shared computer [39];

(d) writing passwords down on a piece of paper (or sticky notes), storing files with passwords digitally on a device (smartphone or laptop) or in the cloud [24,39];

(e) using single sign-on option (e.g., authorization on web sites with Facebook credentials); and

(f) insecurely sharing passwords with others [24,39,49].

To reduce memory load, users also tend to differentiate their accounts depending on their level of importance [39] or the "potential consequences of account compromise" [13, p. 36]. According to these password studies [16,39], most weak coping strategies (such as password reuse and modification or including common phrases and dictionary words) are used for the categories of accounts considered by users of low- to medium-consequence, while accounts of high-importance (such as financial) are treated differently. In particular, users are ready to sacrifice convenience and choose security for accounts with explicit negative consequences of password misuse such as financial loss [43].

The use of Single Sign-On (SSO) presents certain privacy concerns, despite its usability advantages **??**. With SSO, relying parties (the websites that users log into through the SSO provider) are given access to users' personal profile information. Likewise, the SSO provider receives information about its users' accounts from these relying parties. Moreover, users are often not adequately informed about this privacy compromise affecting their accounts. **??**.

In the HCI literature, the existence of these coping strategies is usually attributed to the fact that users tend to minimize the amount of effort they are willing to put into creating and recalling a password, although it may result in less security for their accounts [16,36,43,44]. Therefore, the choice of a coping strategy is influenced by the balance between perceived security risks and usability benefits [24,49]. For example, logging on to shared computers, sharing passwords with others, or reusing passwords have perceived benefits which significantly outweigh the perceived risks for some users in some circumstances. Writing passwords down (in a digital file or on a piece of paper) carries no significant security risks in most cases (since most password attacks are performed remotely) but provides larger usability gains. An increase in the complexity and number of rules for creating passwords imposed on users by the web service often results in a decrease in usability and, consequently, in weaker compliance behavior and increased coping strategies. The requirement of regular password changes can also result in decreased security: this rule often encourages people to reuse their old passwords [49].

Merdenyan and Petrie argued that people generally choose certain password management activities according to their perception of the risks and benefits of such behaviour [24]. In particular, when a user perceives the risks as more important than the benefits, then the likelihood of undertaking the chosen behaviour is reduced by half. For example, in the study, the perceived risks of storing passwords in a digital note on a device outweighs possible benefits and reduces probability that participants undertake this behaviour. Likewise, the likelihood of undertaking a behaviour increases when users see it as primarily beneficial such as in the situation of password reuse where users consider mostly benefits and do not anticipate risks [24]. At the same time, not all users can correctly assess the risks, such as the vulnerability of their password management habits, and predict negative consequences of their actions. Therefore, they may not feel a real need to seek changes in their behaviour to ensure more security [45]. A recent online study from Google indicates that around 70% of respondents (of a representative sample of 3000 adults living in the US) are confident in their ability to protect their online accounts and around 60% believe that their accounts are safer from online threats than the average person's accounts. Herewith, 65% of the same participants reported reusing passwords for multiple or all their accounts (52% and 13% respectively) [15].

The same trade-offs between convenience and security take place when users create their passwords based on their perception of password strength [43, 44, 49]. Ur et al. (2016) conducted an online study comparing users' understanding of password strength and its real ability to withstand password guessing attacks [44]. Most participants demonstrated that their mental models of secure password are consistent with current password policies (such as using random sequences of letters or digits; non-standard capitalization of characters; avoiding password reuse, common words, personal content, or service-related terms). Despite this, they continued performing weak password management behaviours. Tam et al. explain that people "associate secure passwords with a loss of convenience" [43, p. 237]. Their participants emphasized that they do not mind memorizing their passwords, but at the same time they were not ready to put a lot of mental effort into it. When opting for convenience, people are willing to give up security by choosing a password that is easy to remember but less resistant to guessing attacks, and vice versa, when people choose strong passwords, they feel that they are deliberately sacrificing convenience.

2.2 Password managers as tools for secure password administration

To lessen users' cognitive burden associated with secure password management behavior and reduce poor password decisions by users, security experts recommend password managers (PM) as one of the most effective tools for addressing memorability issues and enhancing account security [7, 12, 42]. A password manager is software designed to store and manage online credentials [20, 42]. Experts distinguish three main categories of password managers:

- ***dedicated (or standalone) password managers***[1] [21, 22, 42]. These managers are available either as a software application with an optional web browser extension or as a cloud-based tool [28]. Standalone managers are available from companies that specialize in the development of these tools (e.g., 1Password, Dashlane, LastPass, Bitwarden, NordPass, Keeper and many others) and companies that provide them included in antivirus packages (such as Avast, McAfee, Kaspersky);
- ***browser-based password managers***, which are provided by web browser vendors (such as Google Chrome, Mozilla Firefox, Safari, Microsoft Edge) and are built into the browser [21, 22, 37];
- ***operating system-based password managers***, which are applications built into operating systems [37] (Apple Keychain for MacOs and iOS devices or Samsung Pass for Android devices).

A password manager usually stores a user's passwords and usernames as a database and controls access to this database with a master password [20] or a password to the main web browser account (e.g., password for a Google account if a user manages their accounts in Google Chrome). Therefore, the user has to remember only one

[1] Hereafter, the terms are used interchangeably throughout the text

master password while passwords for each website are saved for them by their manager. To protect user accounts from attacks, modern tools typically store passwords encrypted and salted in the credential database. The passwords can be encrypted and decrypted only with the encryption key derived from the user's master password and username [20].

Depending on the type, password managers offer various features for the management of personal data. Browser-based tools (Figure 2.1) typically include features such as password storing, generating, strength checking, credential synchronizing, auto-filling, and two-factor authentication. Apple Keychain, as an example of an operating system-based manager, also securely stores credit card information and synchronises saved passwords across all of users' iOS devices[2]. Standalone tools (Figure 2.2) offer a variety of more advanced options for password management as described on their websites[3]. These tools are web browser independent and are cross-platform. Most standalone programs provide enhanced mechanisms for password generation such as choosing a combination of characters, numbers, and symbols or giving control over the length of a string. They also offer features such as secure password sharing (e.g., between family members and business contacts), data breach (Dark Web) monitoring, auto-locking, and encrypted storage for non-password data (e.g., credit card numbers, licence keys, personal documentation). Some standalone applications further offer compatibility with Universal 2nd Factor (U2F) devices such as Yubikey (e.g., Dashlane, LastPass), encrypted messaging, VPN, emergency access (Dashline), or travel mode (1Password, Dashline). These advanced features of dedicated password managers are typically offered as a paid subscription (with the basic features available in the free plan), while the other two types of password managers are available for free.

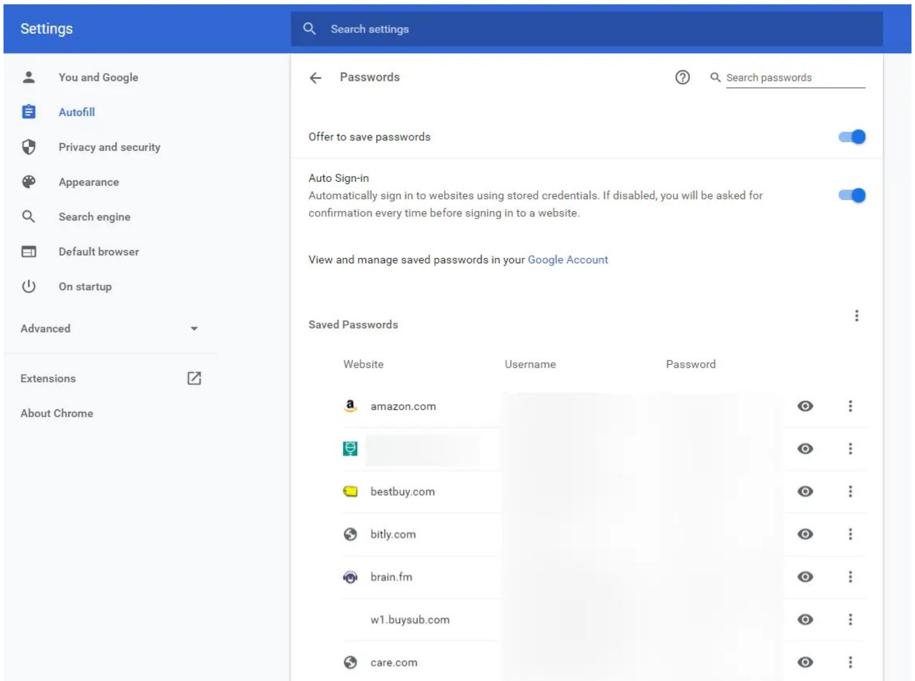
Early studies on password managers revealed significant security and usability

[2] `https://support.apple.com/en-us/HT204085`

[3] A list of password managers available on the market for March 2023 can be viewed here: `https://en.wikipedia.org/wiki/List_of_password_managers`

[4] Photo credit: https://www.computerworld.com/article/3542932/getting-started-with-google-password-manager.html

[5] Photo credit: https://www.pcmag.com/reviews/nordpass-premium



Offer to save passwords

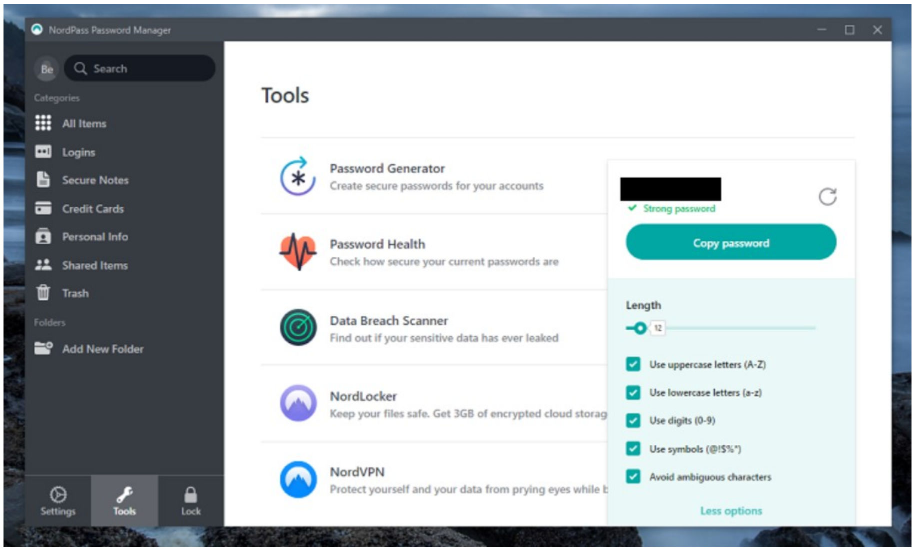
Auto Sign-in
Automatically sign in to websites using stored credentials. If disabled, you will be asked for confirmation every time before signing in to a website.

View and manage saved passwords in your Google Account

Saved Passwords

Website	Username	Password
amazon.com		
bestbuy.com		
bitly.com		
brain.fm		
w1.buysub.com		
care.com		

Figure 2.1: Screenshot of Google password manager as an example of browser-based PM[4]



Password Generator
Create secure passwords for your accounts

Password Health
Check how secure your current passwords are

Data Breach Scanner
Find out if your sensitive data has ever leaked

NordLocker
Keep your files safe. Get 3GB of encrypted cloud storag

NordVPN
Protect yourself and your data from prying eyes while b

[redacted]
✓ Strong password

Copy password

Length 12

☑ Use uppercase letters (A-Z)
☑ Use lowercase letters (a-z)
☑ Use digits (0-9)
☑ Use symbols (@!$%*)
☑ Avoid ambiguous characters

Less options

Figure 2.2: Screenshot of NordPass application as an example of dedicated PM[5]

issues and low manager adoption [7,18]. Recent research [3,28,35] demonstrates considerable improvements in password managers, such as a more user-friendly interface, expanded functionality, and improved reliability. However, password managers are still not widely used; while 65-75% of respondents recognize that they are frustrated by trying to keep track their passwords [15,26], only 22-24% of users rely on password managers [15,31].

Researchers have been extensively exploring the issues of usability, security, and users' acceptance of password managers. Below, we describe these factors in detail and discuss how they can contribute to a significant increase in password manager use. Since many previous studies examined various aspects of password managers, focusing primarily on dedicated and browser-based password managers, this research also focused on the specifics of use of dedicated and browser-based tools.

2.2.1 Security of password managers

A number of studies have examined the security of various password managers in practice, as their possible vulnerabilities can compromise all user passwords at once and diminish users' trust in these tools. Luevanos et al. [21] compared three standalone password managers and found vulnerabilities from clipboard and keylogger attacks, where an attacker can harvest the user's password while the user types in or copies and pastes their password. They also confirmed the need for end-to-end encryption so that server-side attackers do not have access to any of the user passwords. Other studies [20, 37] showed that password managers with browser-based extensions can have insecure auto-filling caused by bookmarklet vulnerabilities where compromised JavaScript extracts passwords auto-filled by a password manager on login pages. They emphasized the need for requesting user interaction through a trusted browser user interface. Li et al. [20] detected some logic errors in credential sharing mechanisms where a password manager (they explored dedicated tools with browser extension) allowed an attacker to create fake accounts and organize compromising communication between these accounts without involving a real user. This study also reported that dedicated password managers are able to successfully mitigate phishing attacks by checking the URL before entering credentials associated with that address and avoiding passwords' autofilling if the page address did not match the original page). Nevertheless, password managers cannot withstand an attack if the tool itself becomes the target of a phishing attack [20].

In a study by Oesch and Ruoti conducted in 2020 [28], the authors assessed vulnerabilities in 13 popular password managers (standalone programs such as KeePass, 1Password, Bitwaden, Dashlane, LastPass, RoboFrom as well as browser-based managers such as Chrome, Edge, Firefox and others). Results indicate that extensive development of these technologies in recent years has led to significant improvements addressing some serious security issues. All evaluated password managers encrypt their databases using AES-256 protocol and employ a key derivation function to transform the master password into a cryptographic key. They have also improved metadata protection, removed insecure bookmarklets, and limited the ability to password autofill on iframes (that previously allowed harvesting attacks). Nevertheless, some serious security concerns were still detected. For instance, several of the assessed tools still automatically enter passwords into untrusted domains without requesting any user interaction, while others require user interaction but allow users to disable this function. Although all password managers evaluated in the study encrypt most metadata, all have at least one item that is stored in plaintext: browser extension settings in 1Password, the website URLs in Chrome, Opera and Firefox, and the website icons in Dashlane. The three browser-based managers (Chrome, Opera, and Firefox) also expose information about account creation data, the time that the manager was last used and the number of password entries.

2.2.2 Usability of password managers

An early usability study of password managers was conducted by Chiasson et al. in 2006 [7]. The study revealed that some important password manager features were so inconvenient to use that the resulting failure of tasks (e.g., incorrect system activation or errors when changing passwords), coupled with a user's misunderstanding of the manager concept, led to serious security exposures. Modern password managers offer a more user-friendly interface and have an expanded set of functionalities, ease of activation, synchronization and use in general, but the research finds that some important functions are still not entirely usable.

Huaman et al. [17] collected user reviews and support requests on the Chrome Web Store and GitHub to analyse the usability of 30 popular password managers (including browser-based and standalone tools). The authors identified noticeable user interaction problems between password managers and websites, such as issues with auto completion and issues working with websites that include complex or non-standard implementations. 40% of respondents from another study [35] reported such usability complaints such as repetitive errors related to autofill and password change features, and a lack of guidance on using password manager functionalities which resulted in longer task completion time (e.g., they were confused about how to set up the tool or generate passwords). Interviews with the participants revealed that they had high expectations from password managers (both from dedicated and browser-based) and, therefore, complained about the lack of features. For instance, some people expected a manager to automatically update passwords in applications or to enable users to use the password generator directly on the website while creating a new account [35]. Participants from a third study also complained about issues when using the tool on multiple devices and problems during the account recovery process [3]. Alodhyani et al's heuristic evaluation [3] of three dedicated password managers (Dashlane, Keeper, and LastPass) showed that the most violated usability principles across all three programs were *Error prevention* and *Help users recognize and diagnose errors*. In particular, there were no "undo" function when saving new changes and the system did not prevent users from storing incomplete passwords or inserting incorrect data in a field.

At the same time, studies indicate improved usability for current password managers. Seiler-Hwang et al. [35] compared the usability of 4 dedicated programs (Dashlane, Keeper, 1Password, and LastPass) and found that the success rate was high for all the tasks (such as initialization, account migration, password change, interaction with native apps) completed on all investigated password managers, while users' cognitive load was low. Alodhyani et al's heuristic evaluation [3] demonstrated high ratings for compliance with Nielsen's usability principles. In other words, the researchers found it easy to copy the password and paste it on the login form, to use the autofill feature for saving time, and to understand the meaning of the icons and terminology used in the system, and they noted that it is not possible to mistakenly modify data without entering a master password. These findings were confirmed through user interviews conducted as the next stage of the same project: effectiveness and simplicity were mentioned as positive aspects of almost all studied password managers (both browser-based and standalone). The vast majority of manager users found it easy to use the tool for authentication and storing their passwords. In addition, most standalone applications users found it very convenient to access their passwords list [3].

The research also shows that the convenience of some specific password manager functions has a positive effect on the security of user accounts. Lyastani et al. [22] identified that passwords entered with a dedicated manager had improved strength and a higher uniqueness rate in comparison with other entry methods (such as Chrome autofill, manual typing or copy-pasting). The increased complexity of passwords stored in standalone programs was associated with the fact that people choose password managers for their benefits in reducing their memory load while offering higher security. As confirmed by Seiler-Hwang et al. [35], those participants who used password managers to generate passwords found the feature easy and useful; the users also reported having more unique and long password strings for their accounts. However, random password generation is used only by half of the actual password manager users [3]: 20% of them randomly generate passwords for a specific subset of accounts and 29% use password generation for each account. The recent study by Oesch et al. [29] explains this phenomenon by the intention of password manager users to avoid the hassle of entering complex passwords manually on devices where a password manager is not installed (e.g., access to Netflix account on Smart-TV). Cross-device password entry is an understudied topic [29], and it is one of the usability issues of modern password management programs.

2.2.3 Intention to adopt password managers

Numerous studies explore the factors that motivate the adoption of password managers [2–4, 12, 32]. *Convenience* and *security* of managers have been identified as the main reasons behind using the tool [2,12,23]. In the study by Alkaldi et al. [2], most participants who installed a password program (90%) chose it due to the convenience the tool provided and 35% of participants indicated that it was installed for security purposes. The authors of another study compared the decision-making process and emotional responses to using, or possibility of using, managers among password manager users and non-users [12]. Having no real experience with the tool, non-users, not surprisingly, did not even mention its usability and convenience as possible incentives to adopt it. While the main factors in favor of password manager among users were convenience (80%) and security benefits (25%). Moreover, the more accounts users had, the higher they rated these password manager benefits.

Interestingly, security is also a significant factor among non-users but as a leading reason for rejecting the tool. For example, non-users were not sure that their credentials can be permanently removed from the password manager databases, worried about losing control of the passwords if their master password was compromised [3], did not trust that managers can keep users' passwords safe, and hesitated in trusting the ability of these tools to protect their accounts [4,12,32]. Non-users also indicated that the high perceived risks from keeping all passwords in one place is one of the inhibitors to using password managers [32]. Overall, research demonstrates that manager users feel more confident as they are more aware of the security and convenience advantages of the tools, while the lack of practical experience in the non-users group makes them more suspicious of its use [12].

User concerns about security relate to the *issue of trust* and a *lack of awareness* of how a password manager works, which significantly affect the behavior of both password manager users and non-users [3, 4, 23]. While half of password manager users (mainly browser-based) from Alodhyani et al.'s study [3] trusted the vendors to store their credentials and delete their passwords permanently from databases, another half of participants from the same group expressed concerns about the tools deleting their passwords and just under half reported little or no trust in vendors. Most password manager users did not fully understand how their passwords are stored and processed (for example, they were worried about losing all their stored passwords or concerned about keeping all passwords in one place). Nevertheless, these concerns did not stop them from using the tool; but these concerns could probably explain why the majority of password manager users in this study saved only a subset of their passwords in managers. The users reported that they only saved credentials for non-critical accounts, choosing the tool mainly for its convenience and ease of access rather than security benefits.

Most non-users identify trust and transparency issues as the major reasons for rejecting password managers. They doubt the security of the tools and demonstrate a lack of awareness of how the technology works; they question whether the synchronization across the vendor's services will work, worry about losing access their passwords if the password manager failed to operate [3, 32], are satisfied with their current approach without use of any managers [23], and are not aware about and how to start using a tool [4]. Some non-users simply do not know about the existence of this technology [23, 32].

People also choose not to use password managers (even though some of them are aware of the benefits of the tool) because of *lack of time* [4,12], *lack of immediacy* [4], and the *perceived excessive effort* required to take action [2, 4]. In particular, 41% of the participants in the study by Aurigemma et al. [4] mentioned that they have more important things to do and cannot allocate time towards choosing, installing, and transferring accounts to a password manager. Also, if people do not perform an action immediately, they simply forget to do it later. In addition, inertia occurs when people are not willing to commit more time and effort than they expected into changing their routine [2, 4].

According to research, *lack of perceived need* and *lack of motivation* are among other determinants of rejecting password managers [4,12,43,44]. About two-quarters of the respondents from two different studies [4, 12] reported that they consider their current ways of storing passwords efficient and do not have concerns about the possible negative consequences of their current password management habits. Therefore, they did not see the need to implement any additional security measures.

To explore factors that may induce non-users of password managers to adopt the tool, Alkaldi and Renaud [2] developed a password manager recommender application for the Google Play store and recruited 470 users, whose task was to install the application, keep it on their device for a week and complete pre- and post-study questionnaires. The application used simple non-controlling language, offered a choice of 3 recommended programs, provided an option to invite users' friends, and highlighted the participating contacts who were already password manager users. As a result of the experiment, 30% of participants installed a program and 81% of those who installed actually started using it. The study findings suggest that the intervention (i.e., prompting the participants to use the application to find and install a proper password manager) facilitated short-term tool adoption, and adoption was noticeably influenced by participants' needs for autonomy and relatedness. In other words, the participants were influenced by their desire to have control over their actions and a feeling of being connected to friends and a larger community.

The positive influence of other people using a password manager was also identified in other study [2]: 26% of participants mentioned that they prefer to wait until one of their close contacts becomes a password manager user before starting to use it themselves. Thus, the *positive influence of friends* or even famous people who started using password managers and *addressing the fear of losing control* over one's choices have been identified as factors that may encourage the tool use. Social influence was also found as a motivator for password manager adoption in another study [23], where more than half of participants from George Washington University were likely to adopt a dedicated program if it was provided for free by their institution.

2.2.4 Comparing dedicated and browser-based password manager users

In 2019, Pearman at al. [32] conducted the first study to investigate differences in behaviour and motivation of real users of different password manager types. The authors compared the password management habits among users of built-in programs (such as browser-based and operating system-based) and standalone applications, as well as among those who use nontechnical tools to manage their passwords. While the majority of built-in password manager users chose to adopt the tool because of prompts from the system and its usefulness and convenience, most of dedicated program users made a deliberate decision motivated by the desire to take control over their passwords' lists and address their security concerns and memory load limitations.

A 2022 study by Mayer et al. [23] confirmed the differences in motivation to adopt two types of password managers: ease of access and use are key factors for browser-based manager users, but perceived security plays a significant role for dedicated program users.

Dedicated password manager users also choose to take advantage of manager features such as password generation and encrypted storage of non-password data [32]. In contrast, many users of browser-based managers do not know how to manage their list of saved passwords and are not even aware of the password generation functionality provided by their web browser. For example, in the study by Mayer et al. [23] only 13% of browser-based manager users reported using this feature compared to more than half of dedicated tool users.

Most Chrome users from another study [3] reported that they use the Google password manager only for storing passwords and do not utilize other available features. They also preferred not to save personal information in Google Drive, while users of dedicated programs from this study actively used the encrypted storage provided by their managers and saved their personal information such as passport or bank details. Dedicated password manager users also tend to combine the use of two types of managers, leveraging each manager as a backup for the other [29].

Despite differences in the reasons for using dedicated or browser-based password managers, representatives of both user groups demonstrate similar behaviour in the way they adopt these tools [32]. Only a few participants who used a dedicated managers noted that they changed all their passwords to randomly generated strings at the time of adopting a program; the majority of both dedicated password manager users and built-in password manager users initially kept their reused and weak passwords, changing them gradually over time.

2.2.5 Mental models in human-centered security

As stated in the previous sections, the lack or incorrect understanding of the password management concept negatively affects user acceptance and shapes users' intention to use it. Users may not fully understand how and where a password manager stores their passwords [1, 3, 4, 12, 32], who has access to the database [3], or how a manager protects their accounts against external attacks [32]. Potential users of password managers may have incorrect expectations of their functionalities [35] or mistakenly consider their current strategies (such as password reuse) to be secure [43, 44], and therefore may not see the need to adopt a tool [4, 12].

In the HCI sphere, a user's understanding of how a system works is called a *mental model* [27, 45, 47]. Mental models are widely considered when improving interactions between a user and a system [45]. Norman [27] emphasizes that the greater the gap between the *conceptual model* (how the system works in reality) and the *mental model* (how the user understands the system), the more discrepancies and failures a user will report. According to Norman, mental models are based on three components: (1) a belief system: how the user's model reflects their beliefs about the system; (2) observability: a correspondence between characteristics of the mental model accessible to the user and the real aspects of the system available to the user; and (3) predictive power: the ability of a user to understand and anticipate the behaviour of the system.

In an ideal world, the user's mental model corresponds to the conceptual model of the system, which leads the person to the correct use of the system [27]. Therefore, when designing mechanisms for security, developers should consider not only the nature of security risks, but also end-users' mental models of these risks, which are tied to different contexts [45]. For example, people may have different mental models depending on the environment (e.g., they consider security differently at home and at work), on the device or operating system they use (e.g., Apple users trust that the Apple store offers only reliable applications), on the perception of hacker attacks (e.g., most people believe that they are not interesting targets for hackers), on the level of expertise (e.g., expert and lay users have different concepts of online security), or on the cultural context (e.g., people may perceive their online privacy differently depending on the country and culture in which they live) [45].

Led by their mental models of online security, people make various security decisions to align their attitudes with their actual online behavior. According to Dourish et al., security is often perceived as an obstacle to normal online routine [10]. Moreover, people perceive protecting themselves against potential security risks to be overwhelming; even those who are confident in their ability to behave safely online do not think they are hundred percent safe because hackers are “always one step ahead” [10, p. 395]). One of the most popular strategies for overcoming ambiguity in trying to stay safe online is delegating responsibility for security [10]. People who trust technology can delegate security management to technology and let the software protect their accounts. For example, some individuals consider it secure to store their passwords in password managers. However, most people do not trust these tools and prefer delegating security to another individual: those who feel that they do not have enough skills to assess technology find it easier to trust another person, such as a knowledgeable colleague or family member, to help with protection. Some people also delegate to organizations (e.g., their employer) or to institutions (e.g., financial institutions which are usually considered highly trustworthy).

Mental models of password authentication define users’ password management behavior. As stated previously, people have different mental models of password strength, account importance, password management strategies, and the consequences of these strategies. Incomplete or incorrect mental models lead people to continue using weak approaches (such as password reuse or creating easy to guess passwords) and increase the chances of exposing their accounts to serious security risks.

To answer our research questions and describe the mental models of password managers in different groups of Internet users, we will consider the users’ perceptions and attitudes towards two types of password managers and views on their password management approach.

Chapter 3

Study 1: Online survey

3.1 Methodology

We conducted an online survey to gauge users' perceptions about different password management strategies and their current approaches. We also wanted to explore the ways users store their passwords and use password management tools. We chose an online survey method to reach a diverse sample of participants from different locations, backgrounds, and demographics, and to collect data for initial analysis of the research topic. The survey also served as a pre-screening tool for recruiting participants for the interview study.

The aim of the online survey was to answer RQ1 and partially RQ2: what are the password management habits in the groups of dedicated password manager users, browser-based manager users, and non-users, as well as what are users' perceptions of browser-based and dedicated password managers?

3.1.1 Survey design

We used Qualtrics[1], an online survey tool, to collect our data. The survey took approximately 15 minutes to complete and consisted of questions about participants' demographics followed by questions about their overall password management habits, and attitudes towards different password management strategies. In particular, we asked participants about (1) the number of accounts they think they have, (2) their perception of the security and convenience of different ways of storing passwords, (3) the strategies they use to store passwords and manage different accounts, and (4) their level of satisfaction with their current approach. The respondents also answered questions about (5) their experience using browser-based and dedicated

[1] https://www.qualtrics.com/

password managers. The questions from (5) served as branching questions and based on the answers, we categorized respondents into three groups:

1. Users of dedicated password managers (who currently use dedicated programs and might also save some of their passwords in browsers).
2. Users of browser-based password managers (who use web browsers for storing passwords, but do not currently use any dedicated tools).
3. Non-users (who do not currently save any of their passwords in any type of password manager).

Each group was asked specific questions about the password manager functionality they use, concerns they have about the two types of managers, and why they chose to use or not use these tools. In our study, we focused on exploring the specifics of using browser-based and dedicated password managers, while the option of operating system managers use was also provided in the questionnaire as one of the methods of storing passwords.

Most of the survey consisted of multiple-choice questions, accompanied by a set of 5-point Likert scale questions that were used to learn about participants' perception of password managers and the level of agreement with some of the statements about the tools. Appendix B shows a full list of survey questions.

The study was granted clearance #116069 (Appendix A) by the Carleton University Research Ethics Board-B (CUREB-B).

3.2 Study participants

We collected 197 survey responses from August 12 to October 8, 2021. We recruited participants using Prolific[2], an online platform for participant recruitment that provides high data quality for online behavioral research [11]. Prolific provides its registered volunteers with recruitment notices for available online studies, and users can choose to participate if they are interested. The respondents were financially compensated after completing the survey (with the reward of 1.88 GBP, or approximately $3.26 CAD), payment was made to their Prolific ID.

[2] https://www.prolific.co

Participants were adults aged 18 and older who could communicate in English. Initially, having received 100 responses, we analyzed the pool of participants on the gender and age distribution and, to equalize the distribution, we carried out additional data collection.

Age	Women	Men	Non-binary
18-20	7 (37%)	11 (58%)	1 (5%)
21-30	31 (50%)	30 (50%)	0 (0%)
31-40	16 (52%)	15 (48%)	0 (0%)
41-50	15 (52%)	14 (48%)	0 (0%)
51-60	15 (54%)	13 (46%)	0 (0%)
61 and older	14 (48%)	15 (52%)	0 (0%)
Total	98	98	1

Table 3.1: Age and gender distribution of the sample

Of the 197 participants, 98 were women, 98 were men, and 1 was non-binary. The participants' age ranged between 18 and 61 and older with the largest group (30%) of age 21-30 years old (Table 3.1). Most of the participants were from the USA (31%) and the UK (25%), 14% from South Africa, 6% - Mexico, 4% - Canada, 3% - Italy and Portugal with remaining respondents from France, Netherlands, Poland, Denmark, and Germany.

3.3 Results

To understand the data and identify common patterns in the responses among the three groups, we performed a descriptive analysis of the data.

3.3.1 Types of users and their password management habits

Respondents were divided into three groups depending on the use of password managers (Figure 3.1). The largest group was represented by users of browser-based password managers and consisted of 127 participants (64% of the sample). 53% of the participants identified themselves as women, 46% as men, and 1 participant identified themselves as non-binary. The group of dedicated password manager users was represented by 39 participants (20%), with 10 women and 29 men. The group of

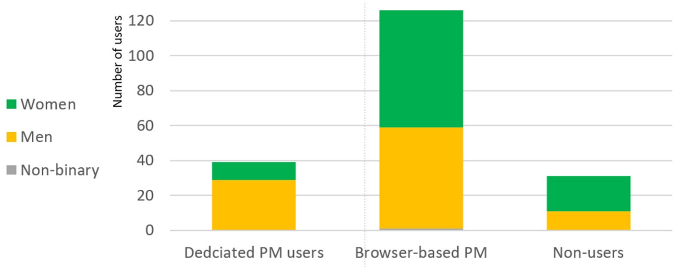


Figure 3.1: Number of participants in each group

non-users was the smallest and consisted of 31 participants (16%) with 20 women and 11 men.

Number of accounts

While most non-users reported having up to 40 accounts in total (29% had up to 20 accounts and 52% had 21-40 accounts), most browser-based and dedicated manager users reported having a larger number, estimating 21-60 accounts (Table 3.2). In addition, among dedicated password manager users more respondents (44%) reported having 61-150 accounts.

Total number of accounts	Dedicated PM users	Browser-based PM users	Non-users
1-20 accounts	2%	10%	29%
21-40 accounts	23%	48%	52%
41-60 accounts	23%	26%	10%
61-80 accounts	18%	6%	6%
81-100 accounts	13%	5%	3%
101-150 accounts	13%	3%	0%
150 accounts and over	8%	2%	0%

Table 3.2: Number of accounts of participants from different groups

As can be seen in Table 3.3, most participants across all three groups assessed themselves as having advanced computer skills. The dedicated password manager users group was the only one that had more users who rated themselves as having proficient computer skills (41%).

Computer skills	Dedicated PM users	Browser-based PM users	Non-users
Basic skills	0%	1%	13%
Intermediate skills	8%	17%	23%
Advanced skills	51%	62%	48%
Proficient skills	41%	20%	16%

Table 3.3: Level of computer proficiency in the three groups

Password storage strategies

We asked study participants about strategies they currently use to store their passwords. Based on previous research [31, 40] and the current state of technology development, we formulated a list of 8 possible methods of storing passwords:

- write down on paper/in a notebook
- save passwords in an electronic file (or digital note) on a device
- save a file with passwords in a cloud service
- send a list of passwords to a user's email
- remember (use memory)
- save passwords in a web browser (such as Google Chrome, Firefox, Microsoft Edge, Internet Explorer or any othe
- save passwords in manager provided by operating system (such as Apple Keychain, Samsung Pass, Microsoft Authenticator, or any similar)
- use a dedicated password manager

Participants rated how often they use each of these methods on a 5-point Likert scale, where 1 meant "I do not use this method to store any of my passwords" and 5 meant "I use this method for all my passwords".

Figure 3.2 summarizes password management approaches among the three groups. In the group of dedicated manager users (Figure 3.2a), the most used strategy was storing passwords in third party password managers (90%), followed by saving passwords in a web browser (87%), memorizing (82%), saving in an operating system manager (67%), and storing passwords in a digital file on a device (51%). The group of browser-based manager users (Figure 3.2b) preferred to remember their passwords

(89%), save them in a web browser (87%), write passwords down in a digital note on device (68%), and save the passwords in an operating system manager (51%). The non-user group (Figure 3.2c) reported only three commonly used strategies: memorizing (87%), writing down on a piece of paper/notebook (61%), and saving passwords in a file or digital note on a device (55%).

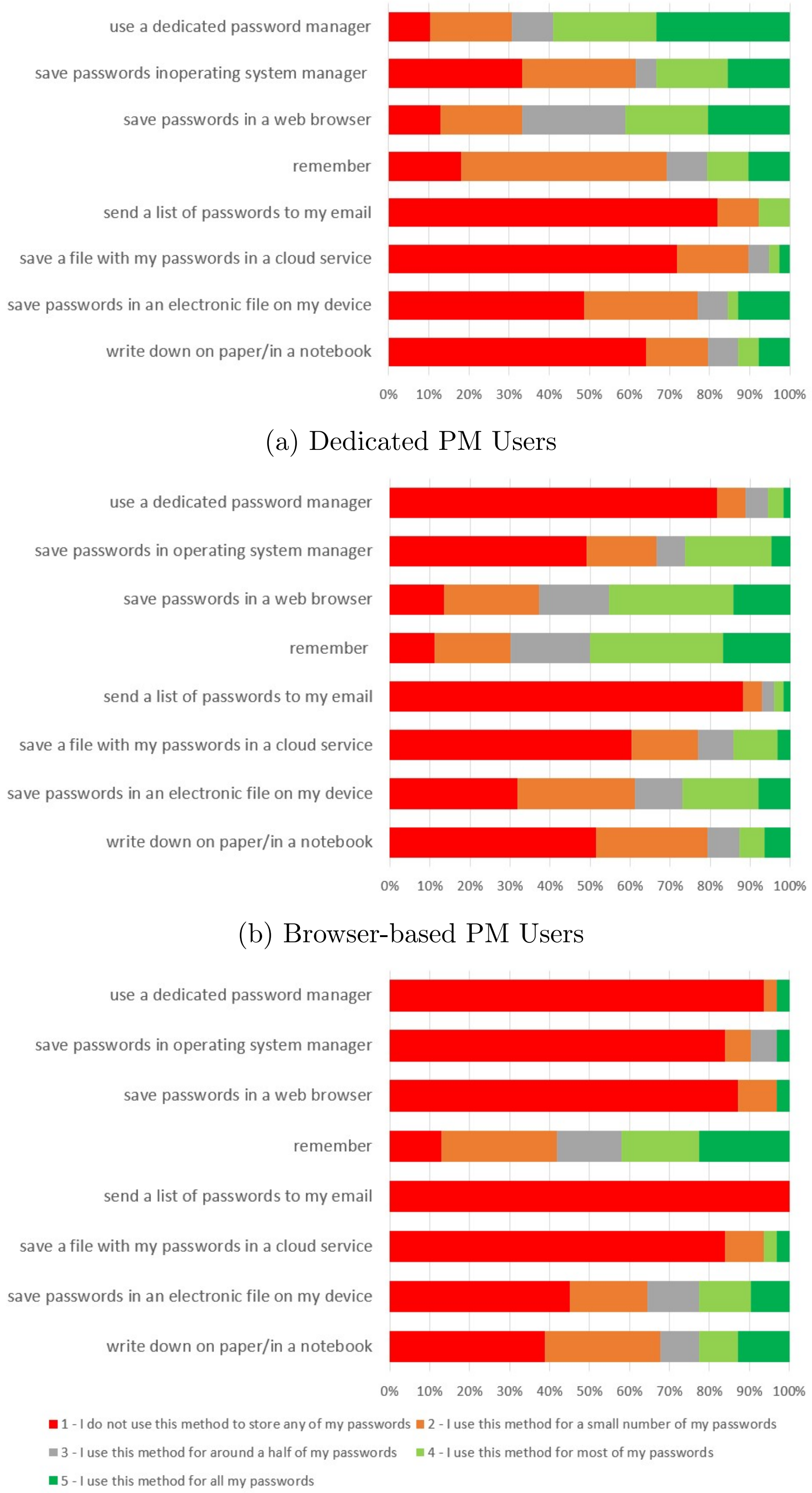
The majority of respondents in all three groups avoided saving a list of passwords in email. Most of them also preferred not to save a file with their passwords in a cloud service. The dedicated and browser-based password manager users preferred not to write their passwords down on paper or in a notebook. At the same time, writing down passwords was the second most popular strategy in the non-users' group.

Even though memorizing passwords was reported as one of the most popular strategies in all groups, we found a pattern that distinguished dedicated password manager users from the representatives of the other two groups. Most of browser-based manager users and non-users preferred to remember at least half of their passwords (the combination of grey, light green, and green bars on Figures 3.2b and 3.2c). In contrast, half of dedicated manager users memorized only a few of their passwords (the orange bar on Figure 3.2a). One possibility is that these were their master passwords for accessing their managers.

Use of browser-based and dedicated password managers

We wanted to understand how people use dedicated and browser-based password management tools in practice and what motivated them to adopt these tools.

Dedicated password managers use Only dedicated manager users answered the questions about the tool they currently use. They indicated the following reasons for using their managers (Figure 3.3). They make password management easier: the tools are considered convenient, they auto-login, and they synchronise accounts across users' devices. Dedicated manager users also chose to use them for security reasons: they strengthen their passwords, store them securely, and provide other security enhancements, such as password generation, password change alerts, or secure storage for non-password data.



(a) Dedicated PM Users

(b) Browser-based PM Users

(c) Non-PM Users

Figure 3.2: Percentage of participants adopting each password storage strategy.

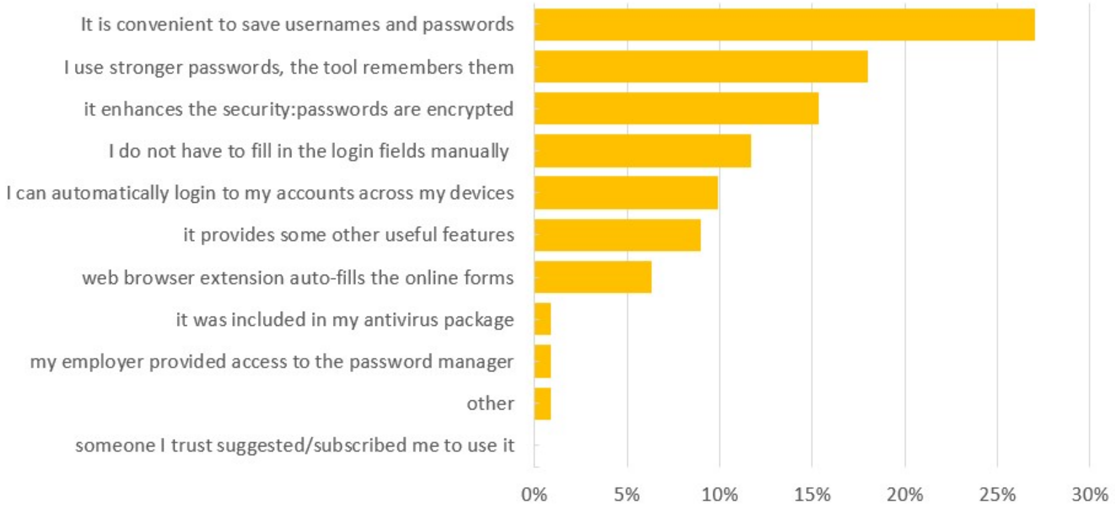


Figure 3.3: Reasons for using dedicated PMs; answered by only the Dedicated password manager group, who selected up to 3 options each.

Browser-based password managers use Participants from both the dedicated and browser-based password manager groups answered questions about the use of browser-based programs. More than half of the participants in both groups named auto-login as the most useful feature of these tools (Figure 3.4), so that users do not have to remember and enter credentials manually every time they need to log in. While the browser-based manager user group mentioned the cross-device synchronization as the next popular reason for using the tool, the dedicated password manager users appreciated the ability to apply stronger passwords for their accounts and the auto-fill feature.

In addition to saving passwords, both groups said their other most used features included (in descending order of popularity): auto-login to online accounts; form auto-filling (e.g., auto-completing names and addresses); two-factor authentication; password checkup for strength and data breach exposure; and synchronization across devices (Figure 3.5).

3.3.2 Perception of current password management strategies

We wanted to understand how participants perceive their current strategies for managing their online accounts. We asked a series of questions about their satisfaction,

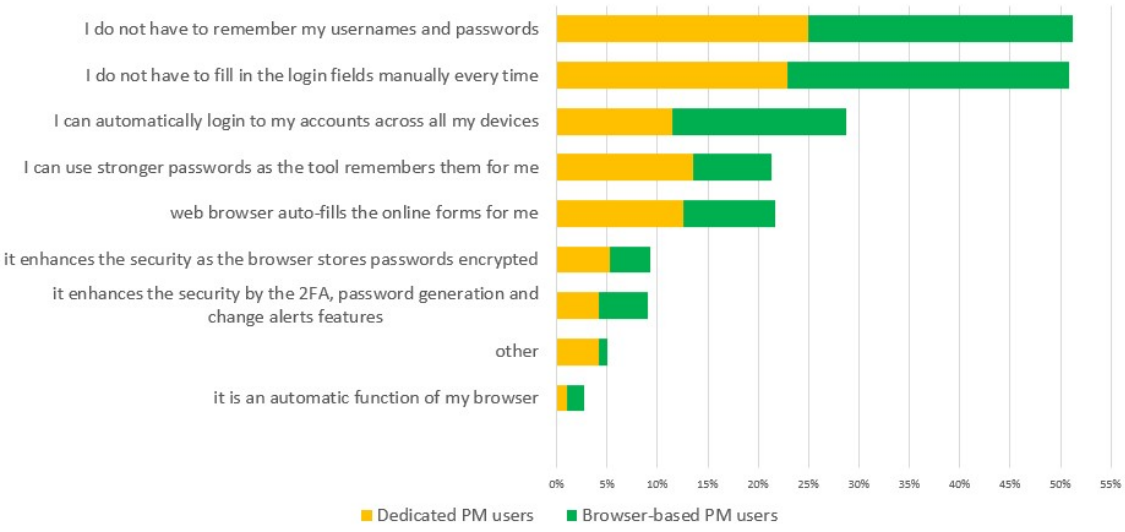


Figure 3.4: Reasons for using browser-based PMs; answered by both the Dedicated and Browser-based password manager groups.

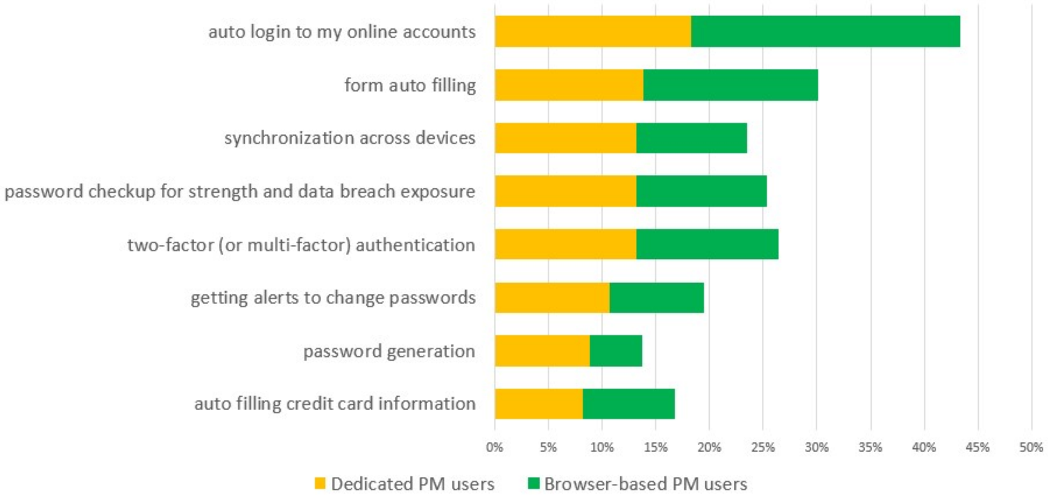


Figure 3.5: Browser-based PM functionality used by the respondents; answered by both the Dedicated and Browser-based password manager groups

perceived difficulty, and security of their approaches.

In general, as shown in Figure 3.6, the majority of respondents from all three groups were satisfied with the way they store their passwords. At the same time, the users from the browser-based password manager group were half as likely to strongly agree that they were satisfied with their current strategy compared to the other groups (23% against 44% and 45% in the groups of dedicated manager users and non-users respectively).

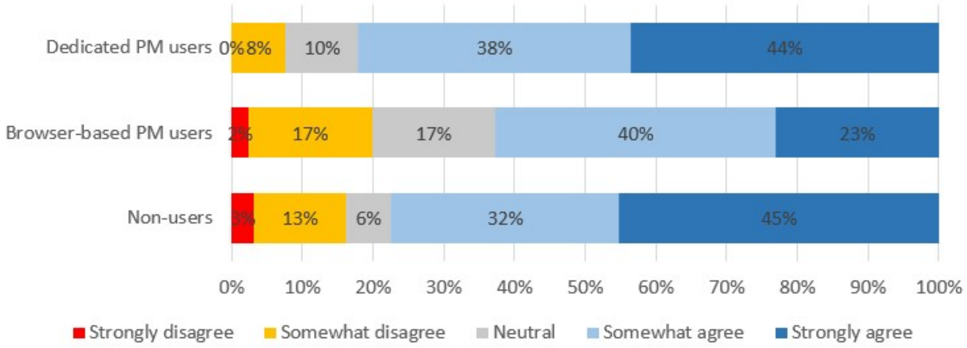


Figure 3.6: To what extent did users agree that they were satisfied with their current password management strategy

We also asked participants to evaluate, on a 5-point Likert scale, the security of their current password management strategy (Figure 3.7). Most dedicated password manager users and non-users expressed confidence in the security of their current strategy (i.e., answered “somewhat agree” and “strongly agree”). In the group of browser-based password manager users, more than half believed they manage their passwords securely.

Browser-based manager users also reported having more difficulty managing their passwords than other groups (Figure 3.8).When we asked our participants about feeling overwhelmed by the need to manage their passwords, dedicated password manager users and non-users reported being less overloaded by this routine (Figure 3.9).

3.3.3 Perception of security and convenience of storage methods

We asked our participants to evaluate different ways of storing passwords for security and convenience by setting two separate questions with a 5-point Likert scale. The

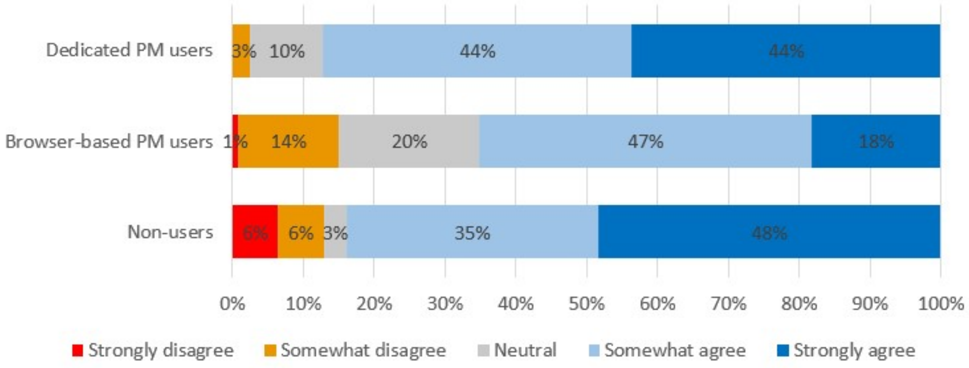


Figure 3.7: To what extent did users agree that they were confident in the security of their current password management strategy

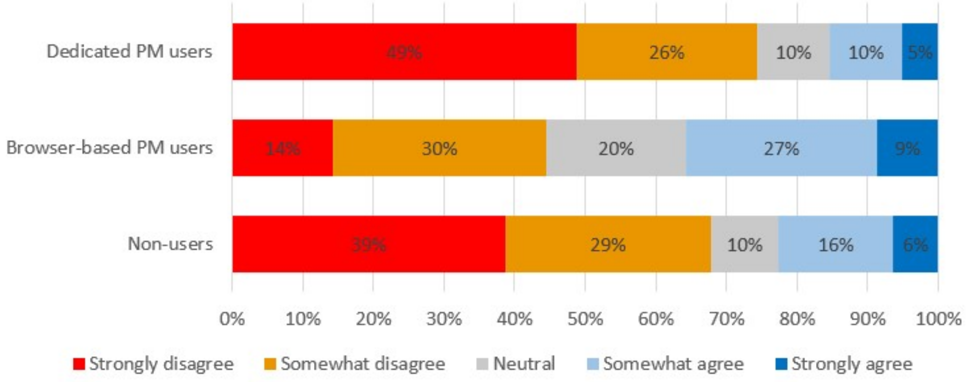


Figure 3.8: To what extent did users agree that it was difficult to manage their passwords

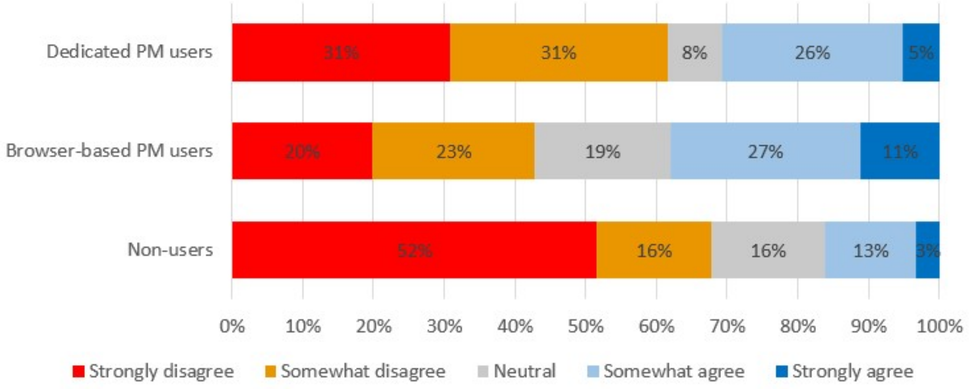


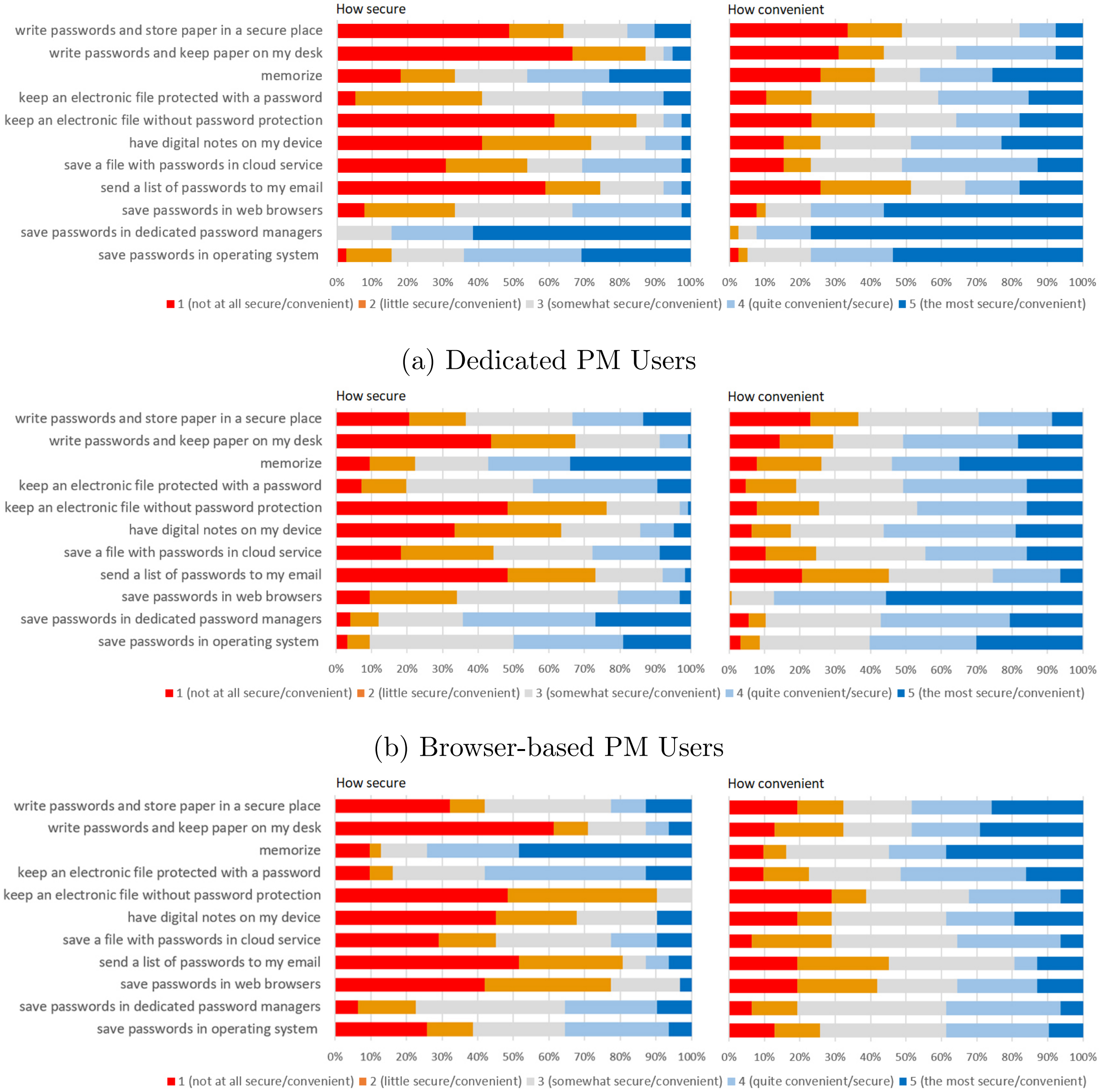
Figure 3.9: Agreement with the statement about feeling overwhelmed by the need to manage passwords.

aim was to understand how users from the three groups perceived different methods of storing passwords and compare this perception with the methods they use in practice.

Dedicated password manager group Dedicated password manager users found the use of dedicated and operating system-based tools to be the most secure and convenient way to store passwords (blue and light-blue bars in Figure 3.10a). Although using browser-based managers was also considered as very convenient by this group (77% aggregated) and was the second most popular strategy (87%), the perceived security of this method was relatively low (33%). Even memorizing passwords, the third most popular method in this group, was considered more secure (46%). In addition, keeping passwords in digital notes on a device, reported as a convenient and popular strategy by half of this group, was also considered insecure (71%).

Browser-based password manager group Storing passwords in web browsers was reported as the most convenient method in the group of browser-based manager users (Figure 3.10b). While this was also one of the most used strategies to store passwords, the security of this method was not considered as the highest in this group: only 20% of users believed it is secure (blue and light blue bars in the Figure 3.10b), compared to the method of saving passwords in dedicated managers (64%), remembering (57%), using an operating system managers (50%), and keeping a piece of paper with passwords in secure place at home (44%). Like the previous group, this user group also preferred to store some of their passwords in digital notes on the device (68%) despite the fact they thought this is insecure (63%).

Non-users group As seen in Figure 3.10c, the most secure and convenient ways to store passwords in the non-user group are considered to be memorizing and having a password-protected electronic file on a device. This is consistent with the way how this group kept their passwords in practice. Writing passwords down, the second most popular method in this group, is also very convenient but perceived to be insecure: 71% thought it is insecure to store a notebook or paper on a desk and 42% thought it is insecure to store it in a hidden place. Interestingly, while this group did not report using any of password managers, more than one third rated operating system and



(a) Dedicated PM Users

(b) Browser-based PM Users

(c) Non-users

Figure 3.10: The perceived security and convenience of different ways of storing passwords

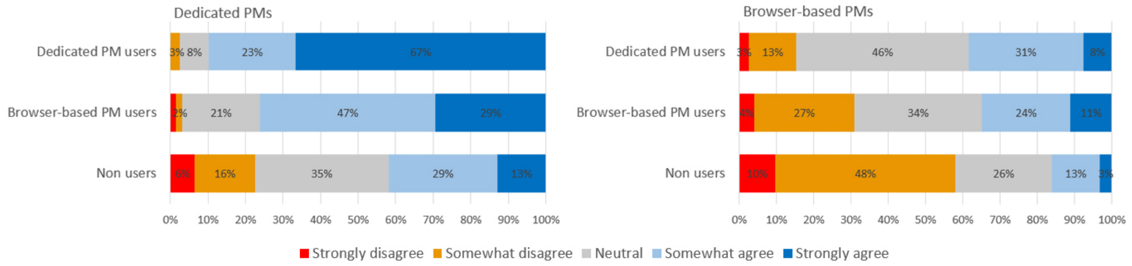


Figure 3.11: Password managers provide extra protection for users' passwords

dedicated password managers as secure (35%) and convenient (38%). But they did not demonstrate any trust in browser-based tools: 77% believed it is very insecure tool for storing passwords.

3.3.4 Perception of browser-based and dedicated password managers

In this section, we investigated perception of various aspects of two types of password managers by all respondents.

Perception of security

Overall, in all three groups, dedicated managers were perceived as more secure than managers offered by web browsers (Figure 3.11). The non-users group showed the greatest distrust of browser-based tools: 58% did not believe it provides extra protection for users' passwords.

We further asked participants more specific questions about their perception of two types of password managers. Respondents of dedicated and browser-based manager users groups believed that web browsers put user data at greater risk than dedicated programs (Figure 3.12). The non-user group believed that both managers put user data at greater risk, disclose user passwords to third parties, and may expose user data to its employees (Figures 3.12, 3.13, 3.14). The browser-based and dedicated password manager users thought that web browser companies are more likely than dedicated manager companies to share user data with third parties (Figure 3.14). But overall, dedicated manager users were the most confident in the security of both types of password managers.

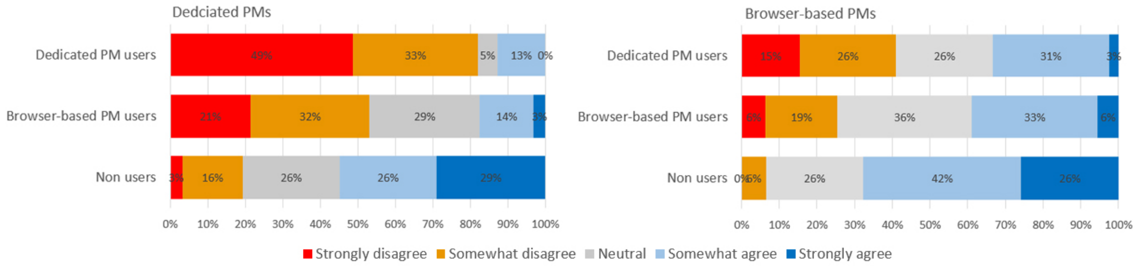


Figure 3.12: Password manager makes user accounts vulnerable to hacker attacks

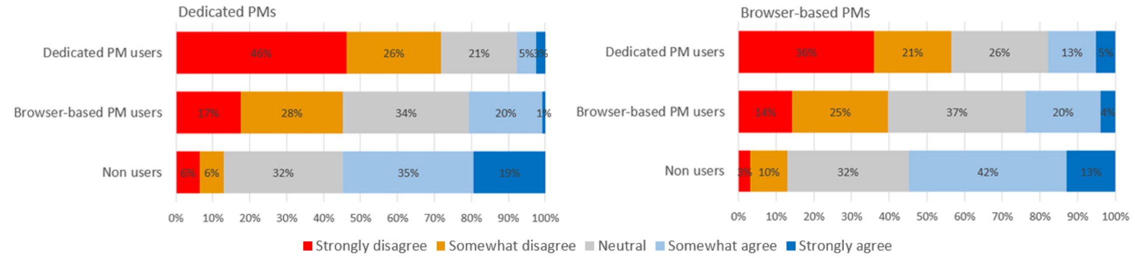


Figure 3.13: To what extent users did agree that employees of company-provider have access to user accounts

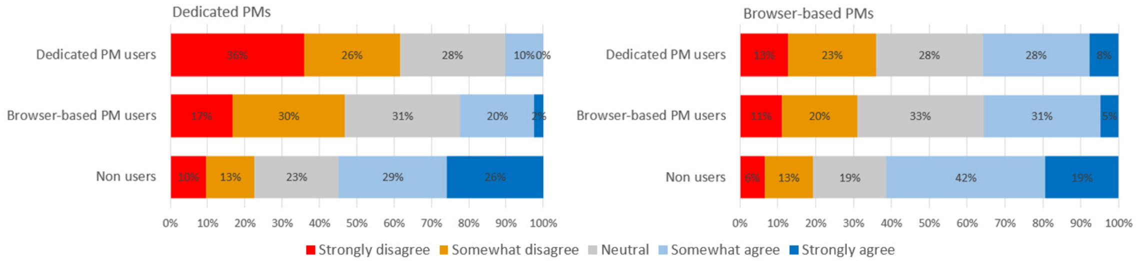


Figure 3.14: User data may be disclosed to third parties

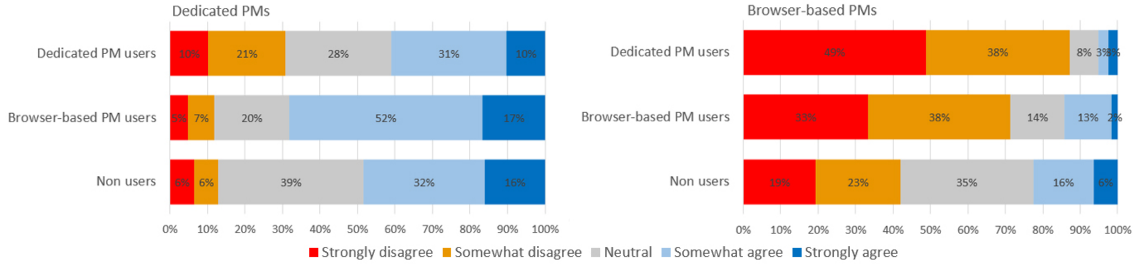


Figure 3.15: Mastering the program requires much time

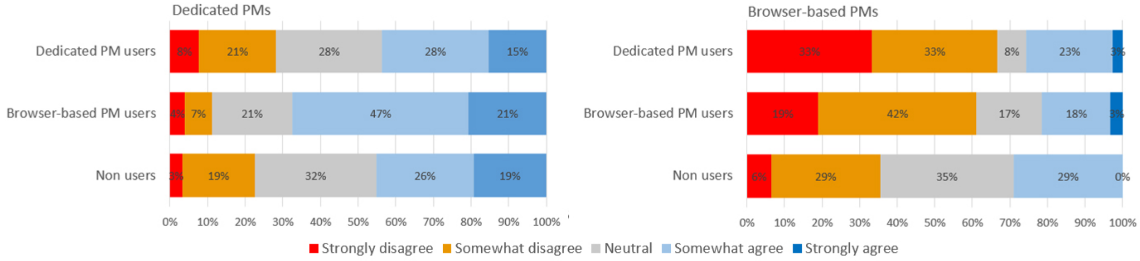


Figure 3.16: Transferring passwords requires much time

Perception of convenience

Participants from all three groups considered both dedicated and browser-based tools as convenient ways to manage passwords, with the group of non-users being more neutral and dedicated manager users being more confident, especially for dedicated programs.

Non-users were also unsure how long it would take to start using a browser-based password manager and transfer all passwords to it (Figure 3.15 and 3.16). The other two groups rather believed that it does not require much time. Regarding dedicated programs, all three groups were more similar, believing that mastering this type of manager requires more time and effort.

Concerns about saving passwords in password managers

Since members of all the groups reported having at least some passwords that are not saved in any type of password managers, we were interested in the reasons for that.

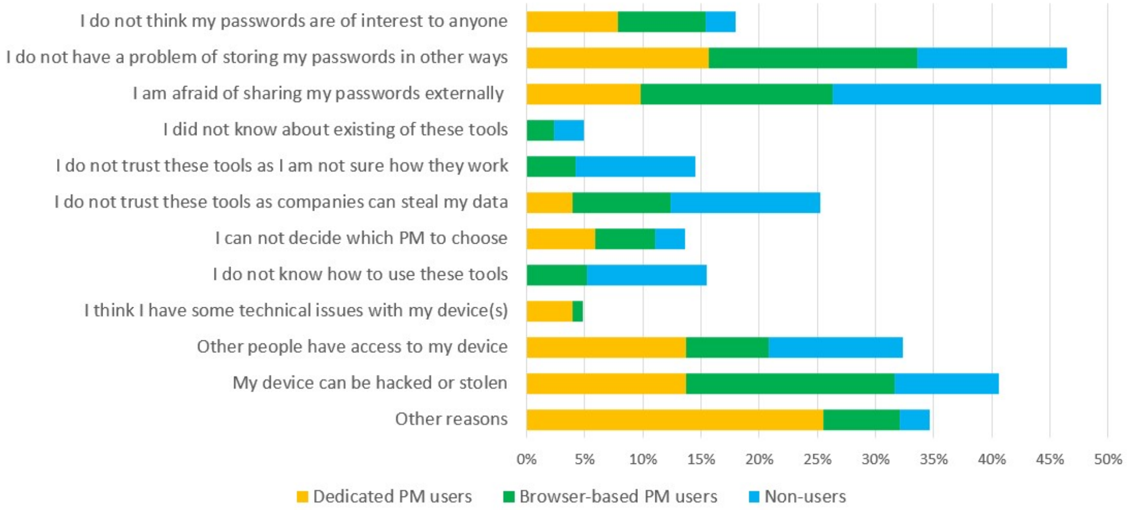


Figure 3.17: Reasons for not saving some user passwords in PMs

It can be seen in Figure 3.17 that 46% of non-users cited lack of trust as their main reason for not using password managers: they were afraid of sharing passwords externally, concerned about how the tool works, and worried about their data being stolen. As well as non-users, the browser-based manager user group expressed concerns about storing some of their passwords externally but not locally on their devices (17%). All three groups had similar concerns about the security of their personal devices: browser-based manager users were afraid that their devices can be hacked or stolen (18%), and the two other groups felt unsafe because someone else has access to their devices (14% for dedicated program user group, 12% for non-user group). In the group of dedicated manager users, one of the reasons for not saving some of their passwords in a manager was the need for storing a master password separately – they have to remember the master password as it gives access to their managers where other passwords are stored.

We further asked the non-user and browser-based password manager user groups about their reasons for not adopting dedicated password managers (Figure 3.18). In the group of non-users, the most prevalent reason was lack of trust in the tool (30%) as these users were not aware how these tools work (17%) and believed that their data can be stolen (13%). Another reason for not using dedicated managers in the group of non-users was lack of knowledge about the tool (25%): some people were aware

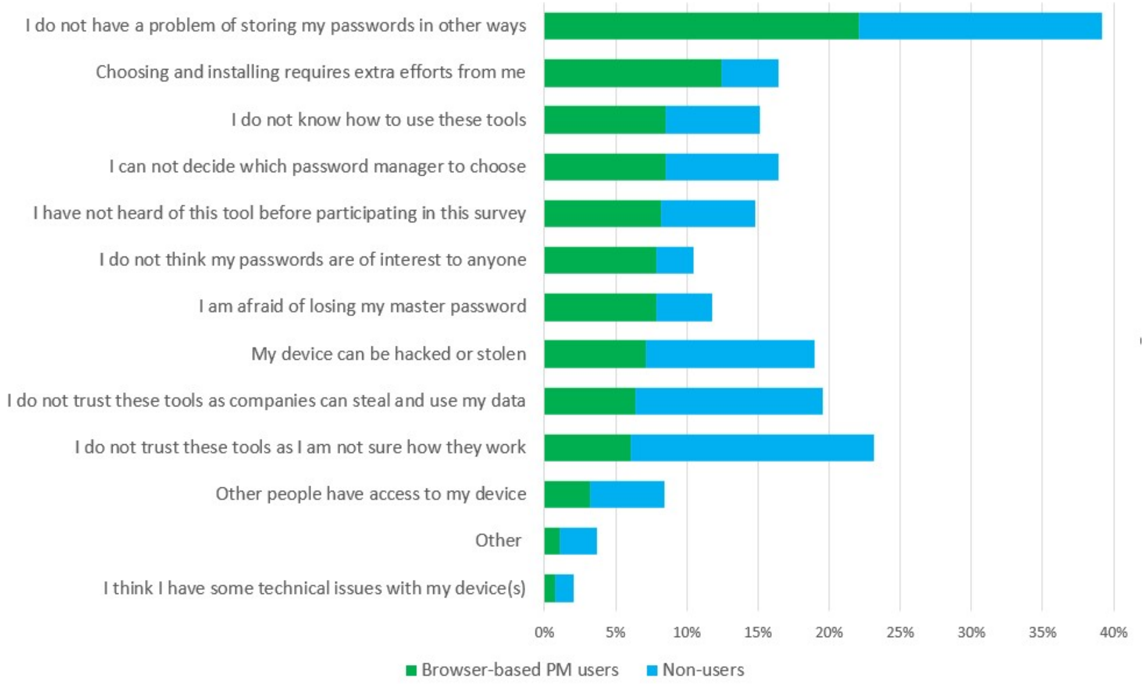


Figure 3.18: The reasons for not using dedicated PMs; answered by both the Browser-based password manager user and Non-user groups

of these tools, but did not have enough time or motivation for researching, choosing, installing, and learning how to use it. Others simply were not aware of the existence of these tools before participating in our survey. 17% of non-users assumed they are safe storing their passwords without special tools. Another 17% did not trust their devices and feared accidental disclosure of the passwords (e.g., if a device is stolen or used by other people who have access to it).

Browser-based password manager users reported a lack of knowledge about dedicated programs as the main reason for rejecting them (38%). Some participants (30%) did not feel the need to use a dedicated password manager: 22% of them believed it is sufficient to store their passwords in other ways, 8% thought no one is interested in their passwords.

3.4 Summary of survey study

The results of the first study allowed us to identify the password management approaches of the three groups, as well as explore their perceptions of dedicated and browser-based password managers.

3.4.1 Password storage strategies

Dedicated password manager users and non-users in general are more concerned about the security of their passwords than browser-based manager users. Both of these groups are satisfied with the way they manage passwords and are confident in the security of their online accounts. But these groups choose different approaches to password management. The dedicated manager user group prefers using special tools to enhance security of accounts such as using third-party, browser-based, or operating system programs. Non-users choose not to use any of these tools, avoid sharing their passwords externally, and prefer to remember them or keep passwords locally (on their devices or in notebooks).

Browser-based manager users seems to be less satisfied with the security of their chosen password management approach and more than others experiences difficulties with the need to manage their accounts. They store over half of their passwords in web browsers, but at the same time evaluate security of browser-based password managers lower than the other methods they use most (memorizing, saving passwords in operating system password manager, or having a digital file on a device).

All groups value convenience, therefore, they use strategies for saving some passwords that are considered more convenient than secure. For dedicated and browser-based manager users, these methods are storing passwords in a digital note on a device even though they are afraid that their devices can be stolen or used by others. Non-users think that memorizing is the most secure way to store passwords, nevertheless they write passwords on a piece of paper or in a notebook or have a digital file with passwords on a device.

3.4.2 Perceptions of password managers

Based on the analysis of attitudes towards the use or non-use of password managers, we identified the perception of two types of password managers among three groups of participants.

Dedicated PM users

Dedicated password manager users demonstrate a high level of trust in third-party password management tools. They consider this type of managers as the most convenient and secure way to store passwords. They argue that dedicated programs allow to have stronger passwords, store them encrypted, and enhance the security of user accounts by providing such features as two-factor authentication or password change alerts. This user group chooses dedicated managers for easy access to their data, password auto-filling, and synchronization user data across different devices. They think that mastering the tool does not require much time and effort. Dedicated password manager users trust half to all of their passwords to third-party tools. Using standalone managers, they only fear losing the master password or are afraid that other people can compromise their accounts by using their devices.

Almost all participants in this group (87%) are also users of browser-based password managers. More than half of this group stores half to all of their passwords in web browsers. Dedicated password manager users think that browser-based managers are convenient, effortless in learning, quite secure tools for storing passwords. They actively use such features of browser-based tools as auto-login, auto-filling, and random password generation. They are aware of how this type of managers works. Nevertheless, they believe that web browsers are more likely to share user data with third parties than dedicated manager companies.

Browser-based password manager users

Browser-based password manager users consider dedicated programs as very secure but not quite convenient for storing passwords. Most of them suppose that it takes much time to learn how to use it and transfer passwords to it. They are not aware how the tool works and do not think they need to learn it. Some of them are distrustful of software provided by the companies.

This group believes that web browsers provide the most convenient way to store user passwords. Most of them store half to all their passwords in browser-based managers for the following reasons: it automatically logs in and auto-fills the user data and synchronizes info across different devices. They also point out that familiarization with the tool does not require much time and effort. At the same time, this user group questions some aspects of the security of the tool: they think that it puts user data at greater risk than dedicated programs and the companies are more likely to share user data with third parties. In addition, this group of users supposes that remembering passwords, storing them in an operating system password manager, or storing them in a digital file is much safer.

Non users

In general, non-users are distrustful of all types of password managers, but they suppose that dedicated programs could be more reliable than browser-based managers. They believe that browser-based tools are especially untrustworthy because web browser companies are more likely to disclose user passwords to third parties than dedicated programs, its employees have access to user accounts, and, in general, web browsers put user data at greater risk. This user group is not aware of how either type of password manager works. They do not know how much time it could take to master these tools and transfer their passwords. They also can not think of a reason to start using these tools as they are satisfied with their current methods of storing passwords. Moreover, this group is afraid that someone can get access to their device so these users have a fear of accidentally exposing the passwords stored in the tool.

Chapter 4

Study 2: Interviews

At the end of the first study, we obtained important information about people's approaches to password management as well as perceptions of their online habits and the use of different tools. In order to discover mental models of password managers and the users' decision-making process, we sought to understand how people distinguish different types of password managers in practice, what types of accounts they manage in browser-based and dedicated programs and why; what passwords they do not store in any tool; how people decide which strategy for storing passwords to use; what might motivate people to start or stop using a password manager. Therefore, the interview study was aimed at answering RQ2 and RQ3: what are the differences in perceptions of browser-based and dedicated password managers in the three groups and what is the decision-making process to begin using or not using browser-based and dedicated password managers in all three groups.

4.1 Methodology

4.1.1 Recruitment

We recruited seven participants in each of the three groups: users of browser-based password managers, users of dedicated password managers, and those who do not use any type of password managers (non-users). The main pool of interview participants was collected through the Prolific platform from those who completed the online survey and gave consent to be contacted to participate in the next stage of the study. As an additional recruiting method, we used personal contacts of the research team to fill the groups. Specifically, with this approach, we were able to find 3 more dedicated password manager users and 4 non-users to make the groups complete.

To contact participants for a potential follow-up interview, we used their Prolific

ID or contacted them via email. To participate in the interview, the volunteers had to be at least 18 years old, be able to communicate in English and agree to be audio recorded. All participants received a compensation of $15 CAD paid via Prolific or direct electronic transfer. The research was granted clearance #116363 (Appendix C by the Carleton University Research Ethics Board-B (CUREB-B).

4.1.2 Interviews

We conducted 21 semi-structured interviews between November 2021 and January 2022. The interviews were conducted online through the Zoom platform and lasted 30-45 minutes. With the participants' consent, all interviews were audio recorded. At the beginning of the interview, the participants were informed that they could skip any question they did not want to answer and stop participating at any time without explanation.

During interviews, we asked in detail about people's password management strategies, perceptions of the importance of different types of accounts, their pain points and challenges in current password management strategies, their perceptions and attitudes towards browser-based and dedicated password managers, their motivation for using (or not using) these and other password tools, and possible incentives for changes in their behaviour (see Appendix D for the interview guide).

The interview recordings were transcribed in Trint[1], a dedicated online transcription software, and manually edited for accuracy. We removed any personally identifying information from the transcript to keep all data anonymous.

4.2 Study participants

Based on the tools they use for password management, we divided the 21 participants into three groups, with seven participants in each group. The first group included dedicated password manager users who installed standalone applications for managing their accounts. They could also use other types of managers such as browser-based or operating system-based and any other means for managing passwords. The second group included browser-based password manager users, who could also practice saving

[1] https://trint.com/

their passwords in other ways but not in dedicated programs. And lastly, the group of non-users consisted of participants who avoided using any type of password managers.

In the group of dedicated password manager users, 4 identified as women and 3 as men. The group of browser-based manager users consisted of 5 men and 2 women. The group of non-users had 5 women and 2 men. The age distribution is shown in the Table 4.1.

Age	Dedicated PM users	Browser-based PM users	Non-users
21-30	1	3	0
31-40	3	2	2
41-50	1	0	1
51 and older	2	2	4
Total	7	7	7

Table 4.1: Age distribution of the interview participants

4.3 Analysis

For the analysis of qualitative data, we chose a reflexive thematic analysis approach. It allows patterned meanings (codes, and later themes) to emerge in the process of working with the data [8]. We found this approach suitable for our goals, as it allowed to move from a descriptive (question-answer) approach to an interpretive one so we were able to uncover the phenomena lying behind our participants' articulated password management habits.

The initial coding was performed by the main researcher by capturing participants' beliefs, attitudes, and values about password related topics. The final code book consisted of 234 codes, which were then grouped into categories according to the main topics of discussion from the interviews. Then we divided all coded files into the three groups of users and performed the initial data analysis by groups. This grouping process helped us to find common patterns in the password management considerations in the three user groups. At the next step, the main researcher and the supervisor met to discuss the overarching themes across all coded interviews, resolve any discrepancies between emerging themes, and update the code book. All themes were considered within the context of the investigated research questions. During discussions the themes were also checked for coherence and richness, i.e., if there was enough meaningful data to support this theme.

The coding process was carried out in NVivo[2], a software package for qualitative data analysis.

4.4 Coding results

In this section, we provide a brief overview of each of our participant groups, based on the codes assigned in our initial coding process.

We started our analysis by creating descriptive codes that reflected recurring password management patterns in each user group. We then divided codes into the 9 following groups: (1) password creation and storing strategies; (2) coping strategies in password management; (3) feelings and thoughts related to password management; (4) understanding of how dedicated managers work, (5) understanding of how browser-based managers work; (6) perceptions and experience using dedicated password managers; (7) perceptions and experience using browser-based password managers; (8) reasons for not adopting password managers; (9) reasons for changing their previous approach. The examples of coding results could be seen on the Figures 4.1, 4.2

4.4.1 Dedicated password manager user group

Overall, having a more sophisticated understanding of online security, participants in dedicated password manager user group tended to practice secure habits. Almost all respondents were aware of the potential negative consequences of careless online behaviour and were afraid of being hacked. Most of them emphasized that being online "you could never be 100% secure" (P4):

> "You never know what's going to happen. My account could still be hacked. Someone can steal my phone, use my fingerprints, and get into a lot of things that can always happen." (P6)

[2] `https://lumivero.com/`

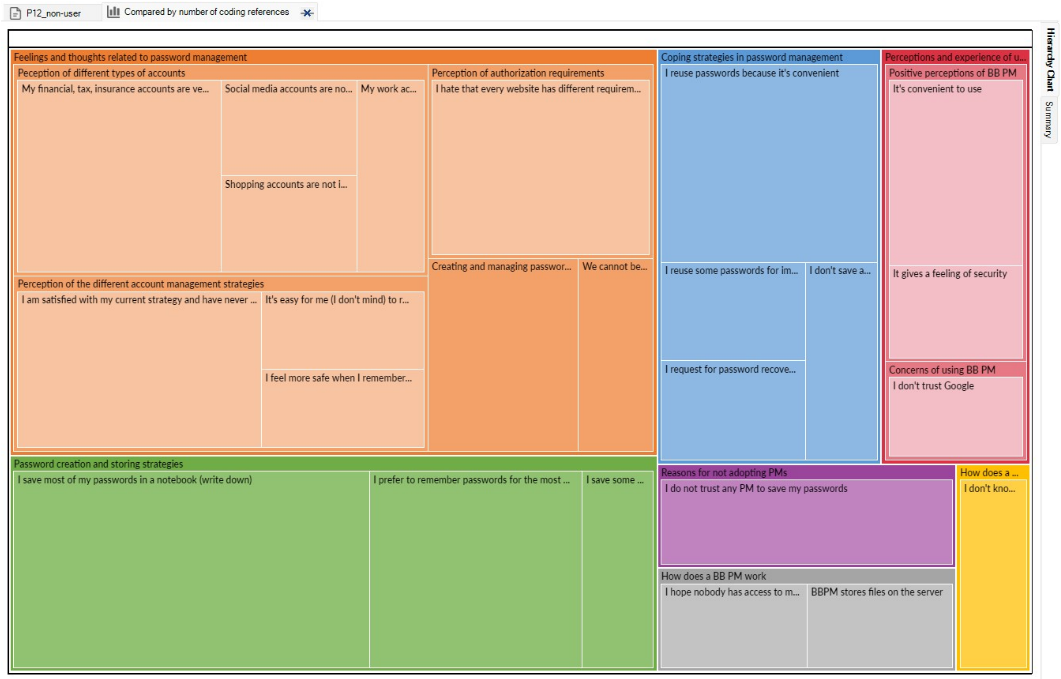

P12_non-user
Compared by number of coding references
Hierarchy Chart
Summary
Feelings and thoughts related to password management
Peception of different types of accounts
My financial, tax, insurance accounts are ve...
Social media accounts are no...
My work ac...
Shopping accounts are not i...
Perception of authorization requirements
I hate that every website has different requirem...
Creating and managing passwor...
We cannot be...
Perception of the different account management strategies
I am satisfied with my current strategy and have never ...
It's easy for me (I don't mind) to r...
I feel more safe when I remember...
Coping strategies in password management
I reuse passwords because it's convenient
I reuse some passwords for im...
I don't save a...
I request for password recove...
Perceptions and experience of u...
Positive perceptions of BB PM
It's convenient to use
It gives a feeling of security
Concerns of using BB PM
I don't trust Google
Password creation and storing strategies
I save most of my passwords in a notebook (write down)
I prefer to remember passwords for the most ...
I save some ...
Reasons for not adopting PMs
I do not trust any PM to save my passwords
How does a ...
I don't kno...
How does a BB PM work
I hope nobody has access to m...
BBPM stores files on the server

Figure 4.1: Hierarchy chart of codes on the example of coding P12 (non-user) interview

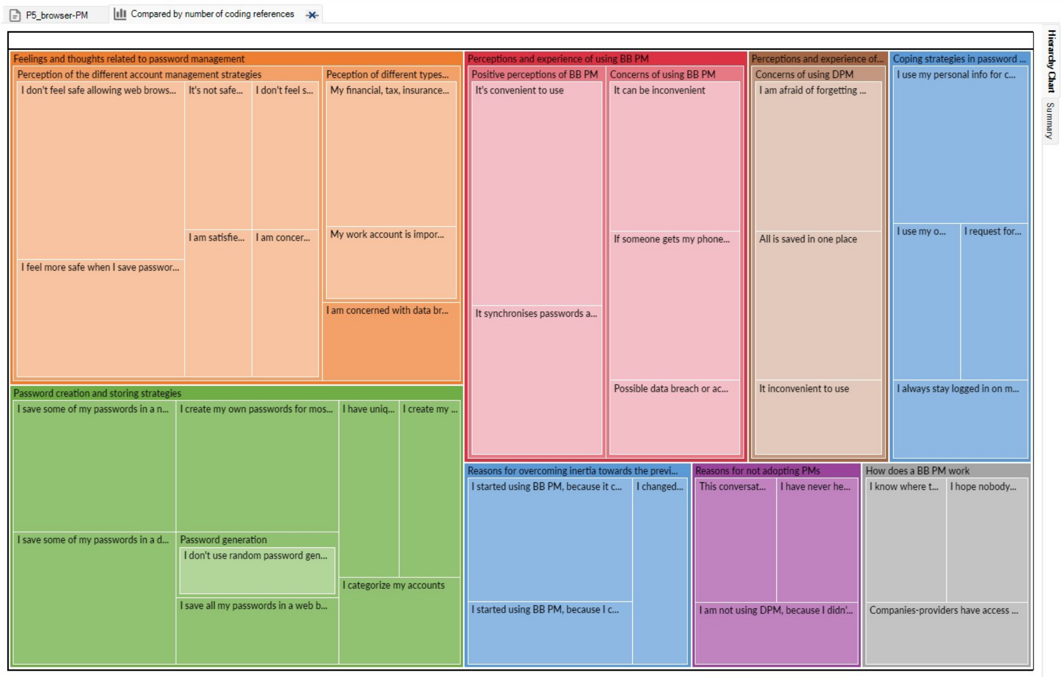

P5_browser-PM
Compared by number of coding references
Hierarchy Chart
Summary
Feelings and thoughts related to password management
Perception of the different account management strategies
I don't feel safe allowing web brows...
It's not safe...
I don't feel s...
I feel more safe when I save passwor...
I am satisfie...
I am concer...
Peception of different types...
My financial, tax, insurance...
My work account is impor...
I am concerned with data br...
Perceptions and experience of using BB PM
Positive perceptions of BB PM
It's convenient to use
It synchronises passwords a...
Concerns of using BB PM
It can be inconvenient
If someone gets my phone...
Possible data breach or ac...
Perceptions and experience of...
Concerns of using DPM
I am afraid of forgetting ...
All is saved in one place
It inconvenient to use
Coping strategies in password ...
I use my personal info for c...
I use my o...
I request for...
I always stay logged in on m...
Password creation and storing strategies
I save some of my passwords in a n...
I create my own passwords for mos...
I have uniq...
I create my ...
I save some of my passwords in a d...
Password generation
I don't use random password gen...
I save all my passwords in a web b...
I categorize my accounts
Reasons for overcoming inertia towards the previ...
I started using BB PM, because it c...
I changed...
I started using BB PM, because I c...
Reasons for not adopting PMs
This conversat...
I have never he...
I am not using DPM, because I didn'...
How does a BB PM work
I know where t...
I hope nobody...
Companies-providers have access ...

Figure 4.2: Hierarchy chart of codes on the example of coding P5 (browser-based password manager user) interview

They were the most knowledgeable group about online security and were able to make an informed choice in favor of using standalone password management tools to maintain their accounts securely. They also used other supplementary approaches such as operating system-based managers and web browsers. Most users of dedicated password manager group recognized the need to have unique and long passwords, many of them had randomly generated passwords, at least for important accounts (like banking, tax services, emails):

> "The fact that my passwords are longer, and more complex, and more random, and never repeat... gives an increased sense of security" (P15)

In this way, they felt protected against guessing attacks and possible data breaches. To enhance the security of their accounts, some users set up two-factor authentication (2FA), changed passwords regularly, and used other security features of their managers.

4.4.2 Browser-based password manager user group

The group of browser-based manager users was more motivated by convenience in their password management choices. They were concerned with the security, but stayed focused on the ways of storing passwords rather the security of the passwords themselves. They felt most comfortable if they remembered their passwords but faced the need to cope with the issue of forgetting them, therefore, participants from this group actively practiced password reuse:

> "Everything from my important accounts to those that are less important to me, the password is the same. It's just the difference in the last digit of the password" (P10)

This group of users was driven by default options in their password management choices. In addition to memorizing passwords as their main strategy, they actively saved passwords in web browsers (but not for critical accounts) and on smartphones. They also wrote them down on paper as a backup:

> "For the important account I just randomly create something that came to my mind on that day. So in that way, that's why I have to write it

> down, because if it's something that I just come up with at that moment, that's why I can forget it" (P5)

4.4.3 Non-users group

The group of non-users seemed to be the most concerned about the risks of being online, many of them felt anxious about the high chances of their data being stolen if it is shared on the Internet:

> "It's just frustrating. I don't want to share anything that can be used against me" (P17)

This fear defined their approach to password management, which was based on the avoidance to save passwords in any online tools. They all believed that memory and paper are the most reliable ways for storing passwords.

This group of users had two distinct subgroups that differ in their approaches to creating passwords. One subgroup actively reused passwords, had short simple strings and found it a great solution to cope with the issue of forgetting passwords. They did not consider this approach to be insecure and did not think that it could lead to their accounts' compromise. For example, even for important accounts, they might have a set of passwords they reused within the certain category or applied slight modifications to the same password they use everywhere (e.g., changing the position of numbers in the same word).

Some participants reported getting annoyed with the need to comply with requirements for creating complex passwords on various web sites:

> "So, what actually drives me crazy when they change the requirements and every website has its own. What I would love to have in this Internet universe and the personal information management universe is that all passwords have same requirements for the complexity, for example, because this makes it easier to reuse passwords that you can remember" (P19)

Another subgroup consisted of people who understood the importance of unique and longer passwords at least for important accounts. They created passwords with the combination of uppercase and lowercase letters, numbers, and special characters. Participants were able to memorize these passwords by having a certain "logical sequence" (P12) or "own strategy" (P14) for creating them:

> "I prefer a combination of words that appear to me at the time and numbers... And with a sign or character. And I always change the words. And, um, for example, for a bank, the passwords for more sensitive accounts, I put a few letters in uppercase and the others in lowercase. For bank accounts I prefer longer password" (P13)

In other words, people from this subgroup of non-users were willing to sacrifice convenience for security by avoiding password reuse and consciously choosing to remember their unique passwords. They were also ready to apply additional security measures to their accounts, such as setting up 2FA and changing their passwords regularly.

4.5 Thematic analysis

The results of our thematic analysis identified three overarching themes that relate to the choice of password management approach by our study participants. These themes are: *complexity of password management strategies*, *perception of control over accounts*, and *inertia*. We also studied our users' perceptions about dedicated and browser-based password managers to be able to build their mental models of these tools. The Table 4.2 shows the example of themes and breakdown of codes by category.

4.6 Theme 1: Complexity of password management strategies

Many of our study participants in all three groups had complex password management strategies, which means they took multiple approaches to storing their passwords. Even in the groups where people used specialized tools, i.e., browser-based and dedicated password managers, only a few participants (who were dedicated manager users) stored all passwords in their manager and used it as the only strategy for maintaining their accounts. Most participants in all three groups utilized 2 or 3 approaches. There were also a few users who saved passwords even in 4 different

Theme	Category	Subcategory	Code	Example Quote
Control over accounts	Perception of different password management strategies	Feeling of security	2FA makes my accounts safer	P3: “I also do that two-step authentication in almost everything I do. You know, people are so vulnerable these days. So it’s up to me to keep everything safe. There’s so much stuff that we, we do online. It’s hard to keep track. So whatever I can do to make it secure, I’ll try.”
Control over accounts	Coping strategies in password management	Password reuse	Passwords reuse for unimportant accounts	P20: “And then I have one password that is like the password that I don’t care. So it’s something meaningless, I use that password because I don’t really care if you hack it because you’re not going to get anything from it.”
Inertia	Strategy change	Dedicated password manager adoption	Inability to manage a growing number of accounts	P3: “Just because it was hard to remember and then I had no categorization of the passwords. They were all random all over the place. So, you know, Netflix password would be beside my banking password. I had no consistency or order... So it was a constant flipping through of pages to find the password if I needed to find it.”

Table 4.2: Example of themes with categories and codes breakdowns with relevant quotes

ways (e.g., remembered, saved passwords in a web browser, digital notes on device, plus wrote down on paper).

Therefore, we were interested to understand why people chose certain approaches to password management, how they understood the security of their accounts, and why PM users did not use their managers as the only way for storing passwords.

4.6.1 Dedicated password manager users group

Most users in this group had straightforward strategies for maintaining their passwords. Two participants managed all their accounts exclusively in a standalone password manager, i.e., utilized only one strategy. They felt certain that the program is secure and valued the benefit of saving all passwords in one place because they needed to remember only one password (their master password). They also did not consider other methods of storing passwords as secure as standalone programs. Other users utilized complementary approaches. Most of them used two strategies: in addition to saving passwords in a dedicated password managers, they stored them either in web browsers or operating system-based managers. One participant had a password-protected file on the cloud.

Avoiding a single point of failure

One of the reasons for adopting two strategies for storing passwords was the assumption of some participants that “putting all eggs in one basket” is not secure. This assumption led these users to finding a supplementary storage for their passwords such as file on Dropbox for P4 or Apple KeyChain for P3 and P21 because they thought these approaches were also secure.

Multiple device compatibility issue

Another reason for not using dedicated programs exclusively was the issue of multiple device use, when participants had their dedicated applications installed on one device only. These participants used free plan which typically allows to choose one device for program installation. They were unwilling to pay for receiving unlimited device use and other paid application features. Therefore, the lack of a dedicated programs on all of the participants' devices provoked them to look for other ways to store passwords if they wanted to access their accounts from devices without a dedicated password manager. So they stored passwords to these accounts in web browsers or operating system-based managers. Moreover, it prompted a few users to practice the insecure habit of password reuse even for important accounts:

> "When I'm logging in through my phone, which doesn't have LastPass, I cannot remember all these passwords, and that's why I'm not even trying to use their random string of characters that they offer. It is convenient to have similar passwords (even for bank accounts – I know it's not the smartest) and I know that nobody's touching my computer... Once the browser offered [to save my bank account], I saved it, and now I'm not even thinking about it" (P2)

Web browsers for unimportant accounts

In the dedicated password manager users group, two users saved the most of their passwords in web browsers. They perceived this tool as secure as their dedicated managers (they trusted Google). They also faced issues with multiple device use of the dedicated tool and for that reason found web browsers more convenient.

However, most participants avoided saving passwords in browser-based managers or saved only unimportant accounts there. These users considered web browsers to be an insecure tool for managing their passwords and felt uncomfortable thinking that user data can be shared with the third parties and the user database can be leaked:

> "If I have a password manager, I will save my passwords there. There's no need to put my password in the place where I don't know it will go" (P4)

4.6.2 Browser-based password manager users group

People in the group of browser-based manager users identified a wide range of password management approaches. Many of them had quite different combinations of strategies, which they explained with their individual rationale for choosing certain approaches. Interestingly, browser-based password managers were not a primary strategy for many participants in this group. Most users utilized three ways of storing passwords. Almost all of them relied on their memory as the main strategy (especially for important accounts) and used browsers as a supplementary approach. The third strategy could be one the following: writing down in a notebook or a digital file on their smartphone, saving passwords in an operating system-based manager on their mobile devices, or remaining logged into applications.

Talking to participants in the browser-based manager group, we noticed that a special role in storing passwords was given to smartphones. People not only stored their passwords as digital notes or screen shots on their phones but also remained always logged into applications (one participant did it even for a banking account).

Memory as the most secure method of storing passwords

The main assumption made by participants in the browser-based manager user group was that to make accounts secure they need to remember passwords well. Therefore, memorizing was considered as the most secure strategy of storing passwords to important accounts. But due to the difficulty of remembering a large number of passwords, most participants tended to create their own easy-to-remember passwords and actively reused them. For example, P11 and P5 included personal information in a password string and reused it across various accounts. For important accounts, they would add a digit or a special character to make a password more complex. P7 and P10 reported having the same passwords that they actively reuse everywhere without categorization:

> “I’ve been using the same password for the last five or six years. It’s more of the same, so it’s easier to remember” (P7)

Only two participants in the browser-based manager user group recognized the need to have unique and long passwords to protect their accounts, but they also wanted to remember these passwords. Therefore, these users created their own “mnemonic structure” (P9) to remember passwords and also relied on 2FA to enhance the protection of important accounts:

> “So, I make big sentences like 15 letters sometimes... I make them funny, they are really funny, so it’s easier to remember” (P8)

Random password generation as insecure and inconvenient method of creating passwords

Having a fear of forgetting passwords and losing control over accounts, most participants in the browser-based manager user group preferred creating their own passwords and avoided use of random password generation provided by their web browsers. First of all, they considered it inconvenient because “it’s impossible to remember like 26 characters of random crap” (P16). Second, some of them supposed it is insecure:

> “I think Chrome gave me an option to say: OK, what about this [random generation of password]? But I don’t. There’s a little bit of trust. I don’t trust it when someone gives me a password, I want to create my own.”

Even if participants used random generation provided by their web browser, they applied it for unimportant accounts only. These could be accounts used rarely (e.g., EasyJet for buying airplane tickets once a year) or used often but without banking or personal information connected (e.g., digital newspaper, online platforms for creating or editing content like Canva).

Web browsers for unimportant accounts

It was surprising to know that most participants in the browser-based manager user group avoided saving passwords to their important accounts in web browsers and used this tool as a backup. Several participants kept some passwords exclusively in their browsers, but these were passwords for the least important accounts they did not want to store anywhere else. Only two users in this group trusted most their passwords to web browsers, including important ones (for email or social media).

Biometric authorization on mobile devices

Many participants in this group associated the security of their online accounts with the biometric protection of their smartphones but not with the password characteristics. These participants emphasized that they have fingerprint protection on their mobile devices, so “no one has access to data on my device” (P7). They felt safe keeping passwords in digital notes (P10, P11), or screenshots (P5) on their smartphones, or remaining logged into their mobile applications (P7, P8, P11). P7 stayed logged in even to their banking account and rarely used such application on their laptop. At the same time, the security issue is that most of these users reported having relatively simple passwords and reusing passwords, which compromises their accounts, no matter how well protected their device.

4.6.3 Non-users group

Having straightforward views on online security, almost all participants from the non-users group utilized two strategies for storing passwords, i.e., their approach was quite simple. All of them wrote passwords down (mainly on paper but some kept the passwords in digital notes on device) and many also memorized passwords to their most important or often used accounts. A few participants mentioned that for the websites they do not think they will use again they might not save the passwords at all and preferred to make a new account or use password recovery next time. Some of them occasionally saved passwords in web browsers, but described it as happening by mistake or intentionally for the web sites they may use “once in a lifetime” (P18).

Extra cautious password management behaviour

Being very careful with sharing passwords anywhere and avoiding use of any online tools for managing accounts, non-users wrote their passwords down on paper. Some of them carefully chose the place to store it at home, one participant even regularly changed the “hidden place”.

Being very cautious, some participants even did not write passwords for important accounts at all, trusting these passwords only to their memory:

> “It is very easy to be hacked. So I think that the most safe place is my mind” (P12)

Smartphone for convenient but insecure management of passwords

Some participants encountered situations where they did not have the paper with passwords with them but needed to have access to one of their accounts. Therefore, for convenience, several participants from the non-users group began to store their passwords in digital notes on their smartphones, although they considered this not entirely secure:

> "I feel more safe to have the passwords for more important accounts saved on the paper only. But life goes on. Sometimes I need to be more flexible. Some passwords for important accounts... they are also in the phone now" (P18)

Web browsers as point of failure for user accounts

Despite having some issues with remembering passwords and the inconvenience of entering them manually, everyone in the non-users group deliberately avoided saving passwords in web browsers because it was perceived as insecure. A few participants had previously used browser-based managers, but stopped doing so after being hacked — they thought the problem was in the web browser, not in their password.

4.7 Theme 2: Perception of control over accounts

When participants in our study described their considerations about online security and explained how they cope with some uncertainties and inconveniences, the theme of control over accounts became salient — they all perceived to be safe if had the ability to control their accounts. But control manifested itself differently across the three groups. Whereas dedicated password manager users and non-users felt being in control by making deliberate choices and taking personal responsibility for security of their accounts, the browser-based password manager users' feeling of control was associated with the comfort of remembering their passwords.

Moreover, in all three groups, there were some participants who were more confident in their ability to protect themselves, while the others, in opposite, could find this responsibility overwhelming and even worrying:

> "I kind of adopted the fear that I could never be free [from taking responsibility] and [it could never be] so easy to do" (P21, dedicated PM user)

4.7.1 Dedicated password manager users group

From conversations with the participants of this user group, it became clear that many of them explicitly felt a need and desire to take control over their accounts:

> "You know, people are so vulnerable these days. Nothing is ever secure. So it's up to me to keep everything safe" (P3)

Thoughtful approach to enhancing account security

This assumed responsibility led most participants in the dedicated manager user group to consciously choose their password management strategy. To make this choice, they had invested time and effort in finding and adopting what they viewed as reliable solutions. So, they started using a dedicated program, transferred their passwords to this new tool, and set up 2FA where it was possible. Some users even intentionally stopped saving passwords in browser-based managers and reduced the amount of personal information shared on the Internet.

Trust in tools and big tech companies

The perceived ability to control the security of their accounts could not have taken place without trust in the tools the participants consciously opted to use. Based on reviews, public posts, and suggestions from close friends, the participants of the dedicated password manager group built their trust in dedicated programs:

> "I guess, [I built trust in 1Password] based on research at the time sort of thing... It was also an action on the part of a family member. I was sure it was a great thing" (P15)

At the same time, when not being able to use their dedicated applications on all devices, these participants had to choose other means of storing passwords in which they also expressed trust and could feel control over their accounts using them. So, some people adopted operating system-based and browser-based password management tools. The choice of these tools was mainly based on assumption about reliability of big tech companies:

> “With Google, I just assume [that as] the biggest company in the world, they probably have really good security. So I just assume that it’s safe because of that and that helps me feel secure” (P6)

4.7.2 Browser-based password manager users group

Participants from the browser-based manager user group were less likely than the others to explicitly talk about responsibility for security of their accounts. Their perception of control over accounts manifested itself in the fear of forgetting passwords - these users felt that they lose control if they do not memorize their logins at least for important accounts. Some felt uncomfortable even if they wrote their passwords down in a notebook or a smartphone as a backup:

> “I suppose it’s more of a knowing that I have passwords in my head. I have a comfort of remembering passwords. I suppose if I was to get a foreign password, that I didn’t know, from the generator, and I would put it in my notes... I’m just so scared to do that” (P11)

Password reuse as a coping strategy

To cope with the fear of forgetting passwords, most participants of browser-based manager user group adopted the habit of password reuse. Only a few participants in this group were able memorize passwords without sacrificing security: they developed a complex system of creating and remembering unique and long passwords for all important accounts:

> “I memorize passwords for like the very important ones. Because even if you hack it, it’s really hard because hacking of 15 characters passwords... consisting of sentences... it takes forever. Nobody’s going to do it. They’re just going to try different account” (P8)

Delegating control to smartphones

Many users in browser-based manager user group also trusted their smartphones. Mobile devices seemed to be convenient and secure storage for various categories of accounts as they belong to the user only, are always available and personalized. Because of built-in biometrics protection, many participants felt in control over passwords saved in smartphones. They stored their passwords in notes or screenshots and remained logged into mobile applications (including banking for some participants):

> "I have a digital file with passwords on my phone because it's a thumb activation, fingerprint protected, so no one can unlock my phone and have this info" (P11)

Less control over unimportant accounts

For less important accounts, people from browser-based manager user group typically followed the default option of saving passwords in web browsers choosing it for convenience and trust in big tech companies that develop these tools:

> "Firefox is a pretty good browsing software, it's like one that cares the most about privacy, I've always liked it. It's a good big company to trust my stuff" (P8)

At the same time, demonstrating trust in browser-based PMs, many people were not aware of how these PM work, and therefore, were uncertain about the extent to which their important accounts are protected:

> "In my head, the browser is a little bit more out there in the in the internet universe than, say, you know, something you download on your computer. So... I don't know if it's completely secure" (P11)

Only a few participants in this group trusted their important accounts to browser-based PMs but no one saved their passwords for banking accounts.

4.7.3 Non-users group

Similar to the group of dedicated password manager users, most participants from non-user group explicitly assumed responsibility for their accounts:

> "Only I can assess my all risks, right? Nobody else. So, when I feel my risks are lower... the convenience, I just choose convenience. If risks are higher, then I choose not to store anything and just remember" (P19)

Loss of control due to saving password externally

Because of huge concerns of being online, the perception of having control for this group was realized through the intention to store passwords exclusively locally (i.e., memorize or write down):

> "Why should I put this information so relevant and so important to me outside of my control? Why? I don't think I should... So, I have a file [on my computer] and this file is password protected. The password for this file is very elaborate. And I know it by heart" (P1)

Therefore, all participants in non-users group were afraid to save passwords in web browsers. Many were very distrustful of browser-based password managers and any other tools for storing user passwords. They assumed that the Internet and technology in general were vulnerable as "hackers are everywhere" and "are looking to hack your accounts" (P13).

A few participants, lacking a basic understanding of how personal devices and the Internet work, felt insecure even using their computer:

> "It's just frustrating. It's just not my thing. I'm not a tech, I'm a hands-on person... With computer, I don't have control over something that can do its own things. You could be in control of a computer if you learn more, but it's not important enough to me to learn how to control it" (P17)

Memory and paper as the most reliable means

Out of a desire to control their accounts, the majority of participants preferred to remember passwords, as "the most safe place is my mind" (P12) and wrote passwords down. They felt safer and in better control if they had a physical rather than a virtual note with passwords:

> "[The] likelihood of a password being stolen from my computer, which is connected to the Internet, is higher then likelihood of a password being stolen from a piece of paper that I keep inside my house" (P19)

Partial delegation of control to smartphones

Like in the group of browser-based PM users, a few participants in non-users group also expressed trust to their smartphones as they have built-in biometrics to control access to their devices:

> "It took me years to have trust in this thing, to build trust in the smartphone I was using. And I knew that I don't think nobody can hack a phone... I don't know, if phones get hacked or not, but I was like, let's save it in my notes" (P14)

4.8 Theme 3: Inertia

In an effort to understand the reasons for the low adoption rate of password managers, we found that one of the causes could be inertia. Inertia is the phenomenon when people prefer to stick to the default option (their status quo) and do not take any action to shift from it until they have a motive to do so [14]. In relation to password management, inertia takes place when people follow their routine behaviour in password maintenance, so adoption of a new (more secure) strategy requires a deliberate change of the existing habits, which, in turn, requires effort and time. P11 describes this:

> "I probably really should just get clean it and start over and have my new passwords, but I'll always go with reused ones... I think it was maybe laziness, and life gets you caught up in things... I do think there could be something that scares us all or we all get hacked that will make us weirdly..., takes a really big push for us to change our behaviors"

From the user interviews, we saw that changes in password management habits' did not happen accidentally, without a "big push" (P11). Password manager adoption always required some intentional action from the users. Dedicated program users discussed the reasons which prompted them to switch to standalone manager use, while many participants from other groups explained why they did not want to turn from current strategies.

4.8.1 Dedicated password manager users group

Overall, the group of dedicated password manager users was a group that could not tolerate the inconvenience of their previous password management strategies, rated it as insecure, and therefore demonstrated the ability to overcome inertia by adopting a dedicated program and changing some other habits. Unlike most browser-based manager users who adopted the option of saving their passwords in the browser as it was provided by default, the users of dedicated password managers had to make a thoughtful decision in favour of choosing the special software and invest their time and effort into transferring passwords.

From user interviews, we identified the three main reasons for overcoming inertia, i.e., for changing the previous password management strategies and transitioning to dedicated programs: the growing number of accounts and the associated inconvenience of the previous strategy; an adverse event, and social influence. We found that these factors can play out on their own, but they also can act as interrelated steps towards behavior change.

The growing number of accounts

The inconvenience of maintaining their growing number of accounts seemed to be the most influential factor influencing a habit change. Most users of the dedicated manager group formerly either wrote their passwords down on paper or tried to remember as much as they could and found it difficult and even annoying:

> "They were all random all over the place. So, you know, Netflix password would be beside my banking password. I had no consistency... So, it was a constant flipping through the pages to find the password" (P3)

Respondents in this group also reported concerns about having simple and reused passwords and the hassle of creating passwords according to different website requirements. Therefore, some of them started looking for solutions for effortless password generation.

Those who previously saved passwords in browser-based password managers were unsatisfied with the security of their accounts and were looking for more reliable means of managing their most important accounts.

In search of the most secure options, all respondents in dedicated manager user group opted for standalone programs. Some of them found it convenient to use a standalone tool for managing all their passwords, while most respondents utilized it in combination with other approaches.

Adverse event

All respondents in dedicated password manager group expressed concerns over a possible data breach on platforms they constantly use. Three participants had an incident where their personal accounts were compromised, one of them even had their credit card falsely charged and blocked due to a stolen credentials from the Airbnb web site. In our group, an adverse event affecting the personal lives and finances of users was a strong incentive to quickly change habits:

> “After I got charged 5,000 dollars for an Airbnb... I started using LastPass, I changed a lot of my passwords, I deleted a bunch of accounts that I knew my credit card was on or that I wasn’t using consistently. I deleted other social media stuff...” (P21)

Social influence

Usually, when people have the need to find a new strategy, they start with some research about existing tools, trying to find solutions on their own. But not everyone ends up with a new strategy after this research. We found that simple advice from a friend served as an ultimate impetus from the outside that prompted a strategy change. Before adopting their dedicated password manager at a family member’s suggestion, P15 had been aware of dedicated password managers for years:

> “I was interested in using it for longer than I’ve been actually using it... Just, you know, taking that day to do the research and switch over, and make the step... Probably also going from always having a free service as a web browser-based versus deciding to pay to do that”

This also happened to P21, when after being hacked and falsely charged, their friend who had already adopted a password manager suggested they listen to podcast about the Internet security and implement their recommendations on adopting password managers:

> “They talked about LastPass and all these strategies... and I actually used the advice that they suggested... I did a little bit of homework research on it and I had positive reviews”.

Social influence was effective when it came by request or as a suggestion from a close friend or relative whom a person trusts. P3 asked their colleague with advanced technical skills for a solution regarding their passwords; P15 and P20 adopted a dedicated program when they were offered participation in a family plan; P6 and P21 received a suggestion from a friend who had already adopted the same strategy.

Another form of social influence was the work environment when people had to use a passwod manager to carry out their work duties. This may influence in favor of using a dedicated programs, if a person found it convenient for work, so that they can start using it for personal purposes too. In our study, P6 adopted LastPass after using Okta in their work environment.

Although the group of dedicated password manager users was able to overcome inertia sufficiently to adopt a new tool for storing passwords, they nevertheless remained under the influence of inertia. For example, P6, P3, and P21 did not change all their passwords when transferred them to a dedicated program and reported having reused passwords which remained from their previous strategy. Also, once choosing a new tool and being satisfied with its performance and security, people become attached to their password managers and can hardly imagine the reasons for changing it:

> “Honestly, I cannot think of any reason that can prompt me to stop using Keeper. It works great, it does its work very well... If only I will know about data breaches... It might be my concern...” (P3)

Interestingly, one participant in this group (P6) stopped using their password manager also by inertia, when they switched to another smartphone device and simply did not install the password manager application again.

4.8.2 Browser-based password manager users group

Inertia, as a tendency to follow the default option, determined the choices of the most users of browser-based manager group. Overall, most of these users have not taken steps to leave the path of least resistance. First, there was always a web browser password manager available as a default option because it automatically offers an easy and user-friendly process for saving passwords. Secondly, the widespread use of smartphones with integrated biometrics contributed to use of the default option where people did not make conscious choices, but rather utilized options provided by their own device. Third, the same passwords that some participants have been using for years were also a result of inertia, as it saves time and effort and does not require any new decisions to be made when creating a new account.

In the context of our research, we were interested to understand why users from the browser-based password manager group do not start using standalone programs and why most of them continue practicing insecure habits (e.g., password reuse, creating easily guessable passwords, keeping notes with passwords on mobile devices). We found that there were two main reasons for inertia in this group: satisfaction with the current strategy and lack of perceived need to increase security.

Satisfaction with the current strategy

Despite some concerns about the security of storing passwords in web browsers, participants in the group of browser-based manager users appreciated the convenience of browser-based tools. They liked the autofill feature of their browsers and easily accessing user accounts from different devices. This was especially valued by those who used web browsers to store most of their passwords:

> “Because when you go online it would automatically ask you: Do you want to store these passwords? When I’m planning to go on this website next time and it says - OK, you have this password. And I was like - Wow! Well, I can get use of it! I use Gmail, so it all is linked and makes everything simple for me” (P5)

Those who preferred to memorize passwords rather than manage all their main accounts with the web browsers likewise valued flexibility in accessing accounts (especially important ones) as they were not dependent on the availability of any tool:

> "If I were to use that other person's device, I can simply log on because I can remember most of my passwords" (P10)

Moreover, the widely used habit of reusing passwords also satisfied people from browser-based manager users group as it significantly reduced the memory overload and anxiety of forgetting them.

The few users in this group who created long and complex passwords and did not reuse them anywhere (despite some inconvenience) were also satisfied with their strategy:

> "My system is probably too labor intensive, but it works well!" (P9)

Therefore, familiarity and comfort with their approaches motivated people to stick to their current options.

Lack of a perceived need to increase security

Interestingly, most of web browser password manager users in our study had not experienced account compromise (or they were unaware of such an incident). Only one participant reported having their account hacked and experiencing negative consequences of financial losses:

> "I used the same password pretty much everywhere as I am really bad about cyber security. I had some accounts stolen. And like for one of my video game accounts, it was linked to my PayPal, so, someone took out 400 dollars" (P16)

But after this incident, they did not make significant changes to their routine, continuing to use an insecure strategy of password reuse even for their important accounts.

Overall the browser-based manager users group had no clear understanding of online security. As we mentioned above, they did not think that some of their habits like password reuse and creating easily guessable passwords could get them into trouble.

They rather preferred to think about ways to store their weak passwords (in smartphones, web browsers, or memory), and were not focused on approaches to make their passwords stronger.

Therefore, having no negative experience with their online accounts and having poor understanding of online security, most users in the browser-based manager group felt safe with their current strategies and did not think they needed more secure password management solutions. We demonstrate this with the example of one participant. P7 used mainly a smartphone in their everyday life. They remained always logged into all applications (including financial) and perceived it as a very convenient approach. They emphasized that their accounts are protected well because of the fingerprint authorization built into the device, so no one can access their smartphone. At the same time, this participant reported having the same password that they reuse everywhere:

> "Well, for me, I've been using the same password for the last five or six years... I think it's easier just for the memory to remember"

So, incorrect understanding of security, combined with satisfaction with the current approach, may reduce some people's vigilance and lead to underestimation of online risks.

We also asked participants from the browser-based manager user group whether they were aware of existing of dedicated password managers as a special software for secure management of online accounts. Most participants knew about these tools. A few participants had even tried one for a while but ended up developing their own strategies for creating and remembering unique passwords instead:

> "At the end of the day, they are safe, they are good, they're okay. But I think I can achieve the same level of security [without them]" (P9)

Those who had heard about dedicated managers but have not tried any argued that they do not completely understand how they work, did not have time or incentive to look for the details, or just "did not think about it" (P16). P11 said:

> "If I'm being honest, it would be laziness and maybe as well not knowing enough about it. Yeah, it would probably be a lack of knowledge"

From conversations with the browser-based manager users, it became clear that knowledge about the existence of dedicated programs does not mean that people understand how they work, nor does it motivate them to learn about the possibilities of that tool. Until they realize the need to find more secure options for managing their passwords, they will not explore standalone password managers' functionality in detail and will not build trust in this tool.

4.8.3 Non-users group

Similar to the browser-based password managers users, non-users were generally satisfied with their approach and believed their approach to be secure. Many participants have been following their approach for years, only adjusting the number and the complexity of passwords to their current needs. More security-aware non-users started learning more about online security and changed their previous password creation and storing habits for more secure ones after having had negative incidents with their accounts. Therefore, this subgroup of non-users demonstrated ability to overcome inertia. However, they did not start using dedicated programs, instead they stopped saving passwords in browser-based password managers and imposed greater restrictions on their online behavior.

Below we discuss satisfaction as the factor that prevents non-users from strategy change. We also consider how adverse events can increase security concerns for some users and motivate a revision of their password management approach. At the same time, we will see how uncertainty about specialized tools and incorrect understanding of online threats deters people from adopting dedicated password managers.

Satisfaction with the current strategy

For most of the non-users, being satisfied with their password management strategy meant being confident that their strategy is secure. By avoiding any online means of storing passwords and keeping them in memory or written down, they felt satisfied. At the same time, they recognized that their approach was inconvenient in some situations:

> “There is not a lot of convenience because sometimes I don’t remember a password...so I have to look at my book...and... it’s a lost time” (P13)

Nevertheless, the non-users felt that lack of convenience was a tolerable price for this feeling of increased security and satisfaction:

> “I know like it’s a very less practical kind of thing I’m doing, but I’m fine with it... I feel satisfied and I don’t have to worry that things might get wrong or if someone hacks or something” (P14)

Some participants expressed frustration with password change requirements or password creation rules on websites when they cannot use their regular unmodified easy-to-remember passwords. Only one participant reported using random password generation to resolve this inconvenience (but for unimportant accounts only) while others who complained still tended to reuse passwords with the same words and number combinations.

Adverse event

Most participants in the non-users group who reported having some of their accounts (e.g., Facebook, Skype or email) hacked belonged to the subgroup of more security-aware people. In response to these unpleasant incidents, the participants began to delve deeper into the topic of online security, changed passwords for important accounts, and made them unique and more complex:

> “So I read a lot about these subjects, one day I decided, okay, this is not clever what I’m doing... I had the same password for everything! It was very easy. Yes, but it’s not safe” (P1)

A few of them also reconsidered the importance of some of their accounts (e.g., social media fell into the category of important accounts) and set up 2FA.

They also started limiting their online presence: they stopped saving passwords in web browsers, reduced the number of online purchases, avoided creating new accounts if it was possible, restricted the sharing of their primary email address on online platforms, or avoided use of their name in an email address.

Thus, as a result of an adverse event, these participants moved from the habit of having reused and simple passwords to more secure ways of managing the important accounts. At the same time, this unpleasant incident did not motivate them to adopt password managers, rather, they switched to non password-related means of increasing security of their online presence.

Incorrect understanding of dedicated password managers

When being asked about dedicated programs, a few participants from the non-user group reported that they had never heard about the password managers and did not show any interest in learning more. Others knew about the existence of these tools, but answered that they do not have enough information to judge their usefulness and security possibilities:

> "I think I read something about password managers last year when I was using this one [from work] and it was such a mess that I wanted to look for some information, but not very... So I can't tell you what I think, because I think I don't have enough information to see things. So I don't know" (P1)

In general, participants in the non-user group were biased against any type of online password management tools. They did not trust any external applications that needed to be installed on their devices because they thought it would make their accounts vulnerable to attacks. One participant did not even save any private information on their computer as they believed that personal computer can be easily hacked remotely. Therefore, the fear of "everything connected to the Internet" shaped these participants' apprehension of dedicated programs: they did not understand how managers are secure and could not imagine the reasons for adopting them:

> "But then in the end, I know that even if I start using the password manager, I might not be even able to sleep" (P14)

4.9 Summary of thematic analysis results

A summary of the thematic analysis results is presented in Table 4.3.

Groups	Complexity	Perceived Control	Inertia
Dedicated PM users	Had straightforward views about online security, most used two strategies for storing passwords.	Felt responsible for the security of their accounts and took a thoughtful approach to enhancing security by having unique and strong passwords, setting up 2FA, and changing passwords.	Overcame inertia by replacing previous insecure password management strategies with the adoption of dedicated programs.
Browser-based PM users	Had different views about online security, a variety of password management approaches, and individual rationale for their approaches. Most utilized three strategies for storing passwords.	Had a fear of losing control over their accounts if did not remember their passwords. Actively reused passwords and delegated responsibility for the security of their accounts to smartphones.	Used default options for managing accounts, were satisfied with their current strategies and saw no need to change them.
Non-users	Had straightforward views about online security, most of them used two strategies for storing passwords.	Felt responsible for the security of their accounts and took a thoughtful approach to making their accounts safe by limiting their online presence, keeping password locally, and avoiding the use of any online tools.	The security-unaware sub-group were satisfied with their current strategies and saw no need to change them. The security-aware sub-group overcame inertia by replacing previous insecure strategies with creating unique passwords and enhancing their accounts' security in ways other than adopting password managers.

Table 4.3: Summary of the themes by the three user groups

Chapter 5

Mental models of password managers

In this chapter, we bring together our survey results with our thematic analysis to identify characteristics of users' mental models of password managers. Based on our three research questions, we outline mental models based on our findings about users' password management habits, their perceptions and attitudes towards password managers, and their descriptions of how they chose to adopt (or not) such tools. We frame our mental models using Norman's three components of mental models [27], and contextualize them with users' perceptions and attitudes around their understanding of password managers.

In both studies, those who were the actual users of one or both types of managers reported their experiences and concerns about using the tools. In interviews, participants who had no experience with these tools were asked about the anticipated benefits and concerns of possibly using the managers.

In all three groups, dedicated managers were considered secure, but requiring effort for adoption. Browser-based password managers were more familiar to all users and were characterized as very convenient but less trustworthy.

As participants within each group generally shared common thoughts about password managers, we describe the mental models of the two types of password managers by group. While the dedicated manager users had well-specified understanding of these tools, the other two user groups lacked knowledge of how the tools work and store user data. Respondents with different perceptions of password managers adopted them differently and made different decisions related to the security of their accounts.

5.1 Dedicated password manager users

5.1.1 Dedicated password managers

The dedicated password manager user group view dedicated managers as essential tools for securely storing and managing their passwords. They believe that these tools use strong encryption to protect their data and assume that dedicated programs are safer than browser-based and operating system-based managers because they were designed with the primary goal of protecting user accounts.

People from this group appreciate the convenience of not having to remember multiple passwords, the autofill features, and the overall seamless interaction:

> "What's nice about it, it is just kind of floating in the background" (P21)

Random password generation is perceived in this group as a function that makes accounts more secure by offering unique and complex passwords. Therefore, many participants from the dedicated password manager user group utilized this feature of their managers for all or at least important accounts. Many also felt protected by receiving notification alerts and the use of such additional feature as secure storage where they saved images (e.g., health card or social insurance number scans), credit card numbers, and other important information.

Standalone managers also allow users to better organise accounts and store them in one place (requiring from its users to remember only one password). These tools are generally trouble free in use and do not require users to learn how to use it.

At the same time, some users face issues resulting from multiple device use, when they do not have their manager installed on all devices. In such cases, they have to cope with this inconvenience by looking for other options of storing passwords, including passwords for critical accounts. Therefore, even being considered as very trustworthy tools, dedicated password managers may not be these users' only way for storing passwords, even for important accounts. For the same reason, not all users from the dedicated manager user group find random password generation convenient:

> "When I'm logging in through my phone, which doesn't have LastPass, I cannot remember all these passwords, and that's why I'm not even trying to use their random string of characters that they offer" (P2)

Dedicated password managers are perceived by many users as applications that should be available for free. It could be related to an association with other commonly used tools for password management, such as browser-based or operating system-based managers, which are offered for free. Unwillingness to pay often was the reason for the described multiple device use issue when individuals chose the free plan which typically allows installation on one device only. However, some participants were ready to pay for additional features:

> "Over a certain size limit [of your storage] you have to pay for a subscription, which I was happy to do. It's not much. The price seemed reasonable to me. And I, you know, I'm sure I got extra things by paying for a subscription" (P3)

When asked about an anticipated experience that might motivate users to switch to another dedicated tool, the common concern was the news of a data breach. Some users also mentioned the significant price change as a potential incentive to look for other options.

5.1.2 Browser-based password managers

Participants in the dedicated password manager user group had previous experience saving passwords in web browsers. However, there were only a few users who kept browser-based managers as one of their current strategies.

They all recognized that web browsers provide a very convenient and user-friendly way to manage online accounts as it is integrated into the browser. But this convenience led most of the participants in this group to consider browser-based tools as less secure than dedicated managers. They believed that their account data was more vulnerable to attacks and can be shared with the third parties when stored in the browser:

> "There's no need to put my password in the place where I don't know it will go" (P4)

Therefore, because of security concerns, most people from the dedicated password manager user group stopped saving their passwords in browsers. They may sometimes use browser-based managers as a backup option or a last resort only for non-critical accounts in case they cannot access their dedicated password manager.

Only two users in this group were trusting of their browsers because they trusted the company-provider (Chrome and Firefox). Browser-based managers, along with dedicated managers, were perceived by these users as equally reliable and more convenient tools, since these managers are available for free and accessible on any devices.

While the actual users of browser-based password managers in the group of dedicated manager users did not anticipate any negative experiences that might prompt them to stop using these tools (other than possible data breach or significant negative change in usability), no other participants considered resuming their use.

5.2 Browser-based password manager users

5.2.1 Dedicated password managers

Overall, the mental model of dedicated password managers among users of the browser-based manager group was likely to be shaped by their expectations about password management tools, as well as their prior experience with these tools.

In this user group most participants were aware of the existence of dedicated password managers, and a few even had limited experiences with them. A few participants learned about dedicated tools only after participating in our study. Only those who had actual experience with dedicated managers could highlight some of the tool's advantages. All of them perceived the managers as a tool that helps users feel more secure.

At the same time, all participants from the browser-based manager user group perceived standalone programs as unnecessary since they relied on other means of storing passwords. They feared forgetting the master password and did not believe that dedicated managers would simplify their online experience. Moreover, they were uncertain about how these tools make user accounts secure and did not appreciate the concept of having "all their eggs in one basket":

> "The centralization of data. It's a common concern. It feels like it's an improved version of having one file with all this data" (P8)

Browser-based manager users were concerned that dedicated managers are designed in the form of separate software. As they believed, this may cause some inconveniences such as issues with installation and updates, as well as multiple device compatibility:

> "So [on your SmartTV] you have to use the remote control to click-click-click to enter the password. It took ages to log in!" (P9)

Additionally, some users were concerned that a program stores user data locally in an application, which potentially leads to troubles if the device is broken or stolen:

> "It looks like that if you lost your phone then that's it, everything [from the password manager app] is also gone with the phone" (P5)

When we asked browser-based password manager users what could motivate them to start using a dedicated program, they usually named reasons or events that are unlikely to happen, such as losing a notebook with passwords, Google data breach, or amnesia.

5.2.2 Browser-based password managers

The browser-based manager user group considered browser-based password managers as a simple and convenient solution for managing passwords. These users typically had a less considered approach to password security. They prioritized convenience over security and valued that browsers offer fast and user-friendly service, with features to remember user passwords and other personal information, as well as autofill and synchronize data across different devices and platforms:

> "You know, it's just... it's there. It's always there. And it's very easy to access and control" (P16)

Most users knew how to access the list of their passwords in browser settings and believed that only account owners have access to user data. A few participants found it difficult to discuss how and where browser stores user accounts. Concerns about the security of browser-based managers, i.e., the fear of possible data breach and the fear that web browser companies share user data with the third parties, led many people not to trust their important passwords to browsers. So, browser-based tools were typically adopted as one of several other strategies for storing passwords.

The auto-filling and auto-login features were one of the main reasons for adopting browser-based managers and using them was perceived as a "life-saver" (P11). Typically, users did not distinguish between these features and considered auto-filling to be a function that auto-fills usernames and passwords to grant access to online accounts. But when using these features, users perceived them as a potential point of failure in the event that their device falls in the hands of an attacker who could gain access to their accounts.

Perceiving browser-based managers as a program, some users believed it can malfunction sometimes which, in turn, causes inconvenience. A few participants reported usability issues where they could not login to their accounts because they thought that the username and the password saved in the browser did not match.

5.3 Non-users

5.3.1 Dedicated password managers

No one among the non-users group had actual experience using dedicated tools, therefore, their mental models are based on expectations about such tools.

People from the non-user group considered standalone password managers as an unnecessary complication for their normal online routine. First, they viewed the process of remembering and writing their passwords down as a minor and unavoidable inconvenience. Second, most of them were unaware of the risks associated with weak and reused passwords, so they felt comfortable sticking to their current habits. But more importantly, most participants of the non-user group had no clear understanding of how these tools work and store user data and they were generally distrusting of any online tool. Therefore, they were very dubious about the security and privacy implications of entrusting their passwords to a third-party service.

As in the previous group, some non-users had concerns that dedicated password managers are provided as applications. They were either reluctant to install another application on their device, or anticipated issues with the application workflow and loss of their data:

> "I have the negative experience about the applications in general, I know what they are working for but they could stop working one day. But if I want to go on to use the information which is inside, what to do in this situation, I don't know. So, in any case, I would need to duplicate [my passwords] in the paper" (P18)

So, even if some non-users could imagine starting to use standalone managers for their accounts, they believed they will never stop saving their passwords the old way. Therefore, standalone programs could not be considered as the only strategy for storing passwords for this group.

When we asked non-users about possible incentives for adopting dedicated password managers, many answered that nothing could convince them to start using these or any other online tools. A few participants identified some reasons like social influence where their employer suggests some application to try, convincing articles or "promotions" (P13) which explain in detail how secure these tools are, or the desire to be "more organized" (P14) and save time.

5.3.2 Browser-based password managers

Most non-users had experience of using browser-based tools, at least when they accidentally agreed to store their passwords in response to a browser prompt. Those who used them viewed browser-based managers as a convenient tool:

> "You just open your browser and click on your whatever account and it opens right away without typing. So, it saves you a couple of seconds every time... ten or 20 minutes a day. So 365 minutes a year!" (P19)

At the same time, they perceived web browser managers as an obvious security risk. Not understanding how these managers work and what online security is, many believed that browsers are insecure by nature, just because "they are online" (P12). Therefore, storing passwords in browsers automatically makes accounts vulnerable. Some non-users even believed that they understand online security more than others, therefore, they assumed that these tools may be used only by people who "think the risk is extremely low or... they don't care [about their accounts]" (P19).

As with dedicated password managers, people from the non-user group could scarcely imagine a reason for them to start using browsers for saving passwords. Only one participant mentioned that "if someone could explain how it works" (P19), they might possibly start thinking about adopting this type of password manager.

5.4 Summary

Based on the analysis of mental models of password managers in the three groups, we suggest that incorrect or incomplete mental models of password managers negatively affect the users' acceptance of the tools or the effectiveness of their use. In contrast, sophisticated mental models of password managers increase trust to the tool and its adoption rates.

Chapter 6

Discussion

In this chapter, we discuss how users' mental models of password managers fit with Norman's definition of mental models [27], the factors influencing adoption of dedicated password managers, and our recommendations for encouraging adoption. We also discuss the limitations of our studies and our proposed future work.

6.1 Norman's components of mental models

Considering mental models of password managers through the lens of mental models as described by Donald Norman can help us to consider the potential weak points of password managers that might hinder their adoption. Norman proposed three components of mental models of any computer system: users' beliefs about the system, observability of the system, and ability of a user to predict the system's behaviour [27].

Users' beliefs The belief system of a user refers to their understanding of how password managers work, which is shaped by their prior knowledge and experience of using the tool, or by their assumptions and expectations about it. In our study, users' belief system about password managers appeared to be tightly associated with their beliefs about online security. Each group of users described distinct perceptions of origins of threats to their online accounts (i.e., weak passwords, devices or programs that have connection to the Internet, lost devices, forgotten passwords). Based on these assumptions, users developed different password management habits as well as different beliefs about the two types of password managers. Those who understood the importance of having strong and unique passwords preferred random generation provided by password managers and believed that managers are able to provide secure storage for their passwords. Other categories of users who were less security-concerned used the same or modified passwords, perceived managers either as unnecessary tool (for dedicated programs) or as a backup for other strategies (for web browser tools), and trusted their memory and smartphones the most.

Observability The observability component of mental models refers to the extent to which the system's behavior is visible to the user. In the case of password managers, on the one hand, most modern tools have user-friendly interfaces and efficient performance [3, 35]. Both dedicated and browser-based password managers provide feedback to their users by having such features as security alert notifications, password generation, password strength checkup, and auto-filling. Dedicated tools make their security features more clear to users (i.e., more observable) by offering such options as secure sharing passwords, encrypted messaging and emergency access.

However, the effectiveness of the implementation of the tool is not clear to the users who cannot observe how efficiently the system is able to do its job, i.e., protect user accounts. In other words, people may not know why they were hacked (or not hacked) — either it was the result of their password management approach, just an accident, or the result of the actions of a third party (such as a data leak on a platform they use). Observability is often an issue for browser-based manager users when they are unaware of the option to manage their passwords in application settings. They might do not know where the list of their passwords is stored, or they discover this location in browser settings by accident. Browser-based manager users are often unaware of its additional security features and use it just as a storage for their passwords. Thus, a lack of understanding of how secure password manager programs are, how they store and organize data, and how people can manage their passwords makes the security aspect of password managers invisible to its users.

Predictability Predictability refers to the user's ability to anticipate the system's behavior. For most users it was easy to expect that their password managers will continue providing convenient and efficient service, for example, fast auto-login, form auto-filling (for both browser-based and dedicated manager users), as well as ease of access to the list of passwords and convenient organization of accounts (for dedicated manager users). At the same time, many users could not anticipate to what extent the system is able to provide security for their accounts and they did not understand the importance of having strong and unique passwords. They would rather rely on their own efforts to protect accounts instead of delegating this responsibility to specialized tools. For that reason, most browser-based manager users in our study did not save passwords for critical accounts in web browsers and mentioned that they were afraid of data breaches. They also did not trust their managers to create random passwords and created passwords on their own. Dedicated programs were perceived as secure tools for password management by their users, who trusted even important accounts to such tools and trusted their manager's ability to protect their accounts. At the same time, some users expressed concerns about possible changes in price for the subscription or significant change in user interface after updates that could make the use of the program inconvenient. These things were something they could not anticipate and that could become a potential reason for switching to another tool.

6.2 Dedicated password manager adoption

Our research examined perceptions of web browser and dedicated password managers by different types of Internet users, as well as their password management habits and the reasons for choosing certain strategies. This allowed us to identify factors driving dedicated password manager adoption. As previous research showed, dedicated programs offer reliable and secure password management solution [28], users of these tools more often use randomly generated passwords and practise more secure online behaviour than others [23, 32]. Below, we describe how individuals who chose dedicated password managers in our study differed from other types of users and discuss their motivation in favor of standalone programs. We also provide recommendations aimed at encouraging the adoption of dedicated password managers.

Correct understanding of online security as the key to safe online behavior While most browser-based password manager users and non-users demonstrated insecure behaviour such as having weak and reused or modified passwords and were coping with the issue of forgetting them, many people in all three groups felt safe and were satisfied with their approaches. They felt able to control their accounts and maintain them securely.

While expressing almost the same impressions of their password management approaches, participants from the three groups demonstrated different behaviours and password management habits. We found that the underlying reason for these variations was in users' *understanding of security* which influenced their choice of password management strategies. Individuals who were concerned about online security, as well as understood the risks associated with weak passwords and the importance of using different passwords for different web sites, reported having long and unique passwords. Most of these people belonged to the dedicated password manager user group and used random generation for their passwords. Many of these security-aware users also enhanced their accounts' protection by applying 2FA. But individuals who lacked a clear understanding of online security had their focus shifted from the password strength to the methods for conveniently and securely storing their accounts. They had lists of passwords in biometric-protected devices or notebooks in secure locations at home but reported having not complex enough and reused passwords.

The combination of clear mental models of online security and standalone password managers drives the adoption of dedicated password managers

We were interested to understand why security-aware people from the group of browser-based manager users and non-users chose not to implement randomly-generated passwords and did not adopt standalone programs.

First, as previous research suggests [44], people tend to overestimate the strength of their passwords and underestimate the ability of guessing attacks (e.g., predictability of common phrases and key patterns). Therefore, it seems likely that these individuals from our study might also overestimate the strength of self-chosen passwords. Second, we found that incorrect beliefs about password managers were also the reason for rejecting the adoption of specialised password management tools by these users. Without correctly understanding how these tools work, people cannot build trust in these tools and properly assess the security and convenience benefits of these programs.

Thus, the adoption of dedicated password managers becomes possible when users have a sophisticated mental model of online security combined with correct understanding of password managers. From our interviews with dedicated password manager users, we can see that the adoption of these tools was typically a response to increased awareness of password security issues and the growing trust in standalone managers as secure and convenient password management solutions.

6.3 Trust in smartphones

In all three groups we had users who reported storing passwords in their smartphones: they remained logged into applications, stored passwords in digital notes, or used operating system-based password managers. In some cases, people were uncertain about which system they used for accessing their accounts and how it works. In the perception of a few participants, the passwords were stored "somewhere" on the smartphone (P11) and if the device was lost or stolen "all passwords are gone with it" (P7).

Dedicated password manager users and non-users utilized smartphones for convenience, flexibility, and as a backup for other password storage strategies. Dedicated manager users also did it due to the multiple device issues with their password managers (i.e., when they had to cope with the inconvenience of having a dedicated program installed on one device only). Users from the group of browser-based managers used their smartphones for storing passwords primarily, as it seemed to them, for security reasons. They described the strong trust they had in their mobile devices because of built-in biometric authorization. Fingerprint and face recognition protection gave them an enhanced feeling of security and they believed themselves to be "the only one who has access to accounts" (P11).

Moreover, most users considered their mobile devices as an invaluable tool for everyday life, which is customized according to their daily demands and available at all times. From this perspective, trusting smartphones for password management could be explained by the perception of smartphones as extension of the self, where the external object becomes part of the cognitive process of an individual [30].

6.4 Recommendations for encouraging adoption

Dedicated password managers offer better control over accounts and provide a variety of more advanced options for secure password management, such as enhanced mechanisms for password generation, secure password sharing, data breach monitoring, auto-locking, emergency access, compatibility with U2F devices. Dedicated password managers also offer encrypted storage for non-password data (such as credit card numbers, licence keys, personal documentation).

We consider dedicated programs to be one of the best solutions for secure and convenient management of user accounts. Therefore, our recommendations prioritize increasing adoption of dedicated password managers, but we also include our thoughts on browser-based managers.

Training and education To target individuals who resist adopting dedicated password management programs and to change their beliefs about these tools, it is important to shift the focus of their attention from the ways of saving passwords to the security of passwords themselves. It is also significant to demonstrate that human memory limitations affecting attempts to memorize passwords could be the largest issue in account security. A possible approach to addressing the issue of easily guessable passwords could be a feature that allows users to ”observe” the weaknesses of some of their passwords, as people may not be aware of the prevalence of some their password generation strategies, such as using common keyboard patterns or replacing letters with numbers (such as “love4you”) [44].

The importance of large institutions in promoting the adoption of password managers Individuals may require more guidance from socially significant institutions about the adoption of password managers to become comfortable with using them. For example, large institutions that users trust (e.g., banks that users trust with their money, or healthcare organizations) may promote existing secure password management solutions. It should be simply explained how online attacks work and how dedicated tools for storing passwords are designed to make accounts safe. A 2022 study [23] demonstrates that educational institutions can be a reliable source of introduction of password managers to its students and staff if the program is offered to them for free. Possibly, organizations might require employees to use password managers as part of their information security protocols, but based on a few participants in our study, this nudging approach does not work for personal use unless users are convinced of the security and convenience benefits of standalone password managers.

Improving password manager features The observability and predictability of managers, especially browser-based tools, could be improved by making the system more transparent. For example, the system could provide prompts which guide users to settings and explain how people can access their saved passwords, tell the users where the manager stores their passwords, how best to maintain them and make them secure. It could also be helpful to provide simple and concise explanations emphasizing the security aspects of the tool that appear on the user path when they encounter the manager or nudge users to try the random password generation feature. Password managers could not only notify their users about attack incidents affecting their accounts, but additionally provide insight into the nature of online attacks and outlining what helped (or didn't help) to withstand an attack.

Since one of the biggest usability issues that users of dedicated password managers face is their use across multiple devices (especially when users have the program installed on one device only), the developers of dedicated password managers might consider including the “all device use” option for free, so that the users may adopt dedicated programs more effectively.

Leveraging trust in smartphones In our study, users seemed to believe that smartphones have security benefits for storing passwords. However, smartphones by themselves cannot increase the security of user accounts, since all passwords that users assume are stored in smartphones are actually stored in the cloud (associated with an application or web browser account), but not locally on the device. This suggests that the trust people hold in their mobile devices has more to do with the affective or emotional significance of these devices to their users, and we suggest that this relationship might be able to be exploited to encourage adoption.

Relying on the phenomenon of trust in smartphones can be beneficial for password manager adoption if designers of these programs consider smartphones to be the default device for storing passwords. For audiences which prefer default options, password management software could be incorporated into smartphones as part of a pre-installed set of applications with the possibility to share passwords with other users' devices.

6.5 Limitations

We acknowledge that our study had some limitations. The data collection for the first study was conducted on an online surveying platform Prolific. The data collection and sampling were limited by methods provided by this platform. In particular, the sampling depended on the respondents' availability on the platform and could be determined by their interests in participating in such studies. We faced this issue when we initially collected 100 responses in August 2021. We noticed that the data were skewed towards female participants of age 21-30 (which was almost 30% of all sample). This abnormality in distribution of age by gender was reported by Prolific as a result of a viral video made by a young female influencer who promoted Prolific as a source of an additional income on a popular social media platform [1]. To equalize age and gender distribution, we set age and gender filters and collected additional data, receiving in total of 197 responses.

The online survey had a limited sample size, resulting in a small number of dedicated password manager users and non-users compared to the dominant group of browser-based manager users (although this most likely reflects the real proportion of password manager users and non-users). For this research, the results of the online survey helped us identify common patterns in the password management habits of different types of users and prepare for an in-depth study of user perceptions in the next study.

The results may also suffer from response bias, when our survey may have attracted participants with higher security awareness about password managers. This could affect the results of the assessment of awareness and use or non-use of password

[1] https://blog.prolific.co/we-recently-went-viral-on-tiktok-heres-what-we-learned/

managers.

At the same time, the complexity of the topic and the general unawareness of users about the specifics of password management tools resulted in detecting some errors in the categorizing respondents by groups. In an online survey, twelve participants, when answering the branching questions, chose an answer that did not reflect their actual password management behaviour. For example, one participant answered that they use a dedicated password manager, but when asked about the name of the manager they use, they named the Google Password manager. This issue was addressed by manually repositioning of these respondents within the sample to the appropriate groups. Nevertheless, there are still some risks that we could not detect all inconsistent cases.

The complexity of the topic could also influence the self-reported data in the interview stage. Participants may not have provided data reflecting their actual password management behavior. Nevertheless, the collected data allowed us to determine recurring patterns and draw conclusions about the underlying phenomena of users' habits.

6.6 Future work

The results of our study suggest a variety of future work.

Our studies had limited sample sizes, and in particular, reached only a small number of dedicated password manager users, and password manager non-users. A future study could seek out a larger sample of these groups, which could be used to provide generalizable statistical findings on differences in password management habits across the three user groups.

Exploring the potential of smartphones as a trusted device that may encourage the adoption of password managers also represents an area of future research. In our study, we found that even in the most distrustful of any online tools group of non-users, there were cases of using smartphones to store passwords. Therefore, future research could involve non-users in use of dedicated password managers on their smartphones. It could aim to evaluate the extent to which non-users' mental models of password managers have changed after participation in the study. To expand the studied audience, the future research could involve both browser-based password manager users and non-users, offering them a dedicated program trial.

Upon identifying that users of browser-based managers avoided storing passwords for critical accounts in their managers, as well as remained uninformed regarding how browser-based managers operate and safeguard their passwords, we suggest that this audience emerges as a promising area for future research. In a 2020 study, Alodhyani et al. [3] emphasized that the lack of transparency of browser-based managers and the unawareness of users about what happens to their stored passwords hinders the effective adoption of such tools. This issue has not yet been addressed, and future research may focus on exploring how development of browser-based managers' features can increase current users' trust in the tool.

Chapter 7

Conclusion

For secure and convenient management of online accounts, experts suggest adoption of password managers, specialized tools that help users securely store and organize their passwords. The main goal of our research was to explore users' mental models of browser-based and dedicated password managers (which have lower adoption rates).

To investigate mental models of password managers, we conducted two studies: an online survey followed by an interview study. For these studies we set up three research questions which help to explore different aspects of mental models:

RQ1 What are the password management habits in three groups of Internet users:

- users of dedicated password managers
- users of browser-based password managers
- non-users

RQ2 What are the differences in perceptions of browser-based and dedicated password managers in three groups?

RQ3 What are users' decision-making processes for using (or not using) password managers in all three groups?

Addressing the Research Questions In our online survey study with 197 participants, we collected information about the password management habits (**RQ1**) and perceptions of password managers (**RQ2**) for the three groups. We found that dedicated password manager users adopted dedicated programs along with other methods of saving passwords, such as browser-based and operating system-based managers. On the other hand, browser-based manager users preferred to memorize their passwords and save them in smartphones, using web browsers as a backup. Non-users memorized and wrote their passwords down, avoiding use of any online tools. We also asked respondents about their perceptions of password managers. The dedicated manager users group perceived both types of password managers as secure and convenient. The browser-based manager users group thought that browser-based tools provide a convenient but not very secure solution, while dedicated programs were considered secure but not convenient because of the require time and effort needed for researching alternatives and learning how to use them. Non-users thought that both dedicated and browser-based managers were very convenient but insecure.

To get more detail into users' motivations and decision-making processes (**RQ3**), as well as perception of password managers (**RQ2**), we next conducted a set of semi-structured interviews with 21 participants. Our thematic analysis helped us identify three themes affecting how people use and adopt password managers: (1) complexity of strategies, (2) control over accounts, and (3) inertia.

Describing mental models Together, the results of our two studies allowed us to describe the mental models of dedicated and browser-based password managers from the perspective of the three user groups. We found that users' mental models of password managers combined with their perception of online security played a significant role in influencing their password management choices. The dedicated password manager user group preferred to generate random passwords, had unique passwords for at least important accounts, relied on dedicated programs to store and organize their accounts, finding these tools convenient and secure. However, they deliberately avoided saving important passwords in web browsers because these tools were considered less trustworthy.

The browser-based password manager user group was less aware of the importance of having strong passwords, actively reused or modified passwords to cope with a fear of forgetting them, and preferred to choose the default options of saving passwords in web browsers. They considered browser-based managers to be a simple and convenient solution for managing passwords but did not trust browsers to save passwords for their critical accounts. They did not believe dedicated managers to be essential for enhancing the security of their accounts, and rather relied on their smartphones to save passwords, believing that they were protected by the biometric authentication on their devices.

Non-users seemed to be the most security-concerned, were distrustful of any online tools, relied on their memory the most, and were ready to suffer for security. One subgroup of non-users was more security-aware; they tended to create unique passwords for important accounts and enhance account security in other ways. The other subgroup of non-users actively reused passwords and was overwhelmed by the need to comply with different password creation requirements on web sites.

Recommendations Based on our findings, we made recommendations for increasing the adoption of password managers in audiences who currently reject their use and who have incomplete mental models of online security and password managers. We suggest leveraging the trust and popularity of smartphones among users, and recommended that large organizations, such as educational institutions, take an active role in promoting the adoption of password managers.

Bibliography

[1] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? 2016.

[2] Nora Alkaldi and Karen Renaud. Encouraging password manager adoption by meeting adopter self-determination needs. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[3] Fahad Alodhyani, George Theodorakopoulos, and Philipp Reinecke. Password managers—it's all about trust and transparency. *Future Internet*, 12(11):189, 2020.

[4] Salvatore Aurigemma, Thomas Mattson, and Lori Leonard. So much promise, so little use: What is stopping home end-users from using password manager applications? 2017.

[5] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567. IEEE, 2012.

[6] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. Passwords and the evolution of imperfect authentication. *Communications of the ACM*, 58(7):78–87, 2015.

[7] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, volume 15, pages 1–16, 2006.

[8] Victoria Clarke and Virginia Braun. Successful qualitative research: A practical guide for beginners. *Successful qualitative research*, pages 1–400, 2013.

[9] DashLine. Dashlane study: Us internet users drowning in online accounts – with further tidal wave approaching. 2015. `https://www.prweb.com/releases/2015/07/prweb12860738.htm`.

[10] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, 2004.

[11] Peer Eyal, Rothschild David, Gordon Andrew, Evernden Zak, and Damer Ekaterina. Data quality of platforms and panels for online behavioral research. *Behavior Research Methods*, pages 1–20, 2021.

[12] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, 7(1):1–20, 2017.

[13] Dinei Florêncio, Cormac Herley, and Paul C Van Oorschot. An administrator's guide to internet password research. In *28th Large Installation System Administration Conference (LISA14)*, pages 44–61, 2014.

[14] David Gal. A psychological law of inertia and the illusion of loss aversion. *Judgment and Decision making*, 1(1):23–32, 2006.

[15] Google and Harris Poll. Online security survey. 2019. `https://services.google.com/fh/files/blogs/google_security_infographic.pdf`.

[16] Cormac Herley and Paul Van Oorschot. A research agenda acknowledging the persistence of passwords. *IEEE Security & privacy*, 10(1):28–36, 2011.

[17] Nicolas Huaman, Sabrina Amft, Marten Oltrogge, Yasemin Acar, and Sascha Fahl. They would do better if they worked together: The case of interaction problems between password managers and websites. In *42nd IEEE Symposium on Security and Privacy, IEEE S&P 2021*. IEEE Computer Society, 2021.

[18] Ambarish Karole, Nitesh Saxena, and Nicolas Christin. A comparative usability evaluation of traditional password managers. In *International Conference on Information Security and Cryptology*, pages 233–251. Springer, 2010.

[19] Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas. Security keys: Practical cryptographic second factors for the modern web. In *International Conference on Financial Cryptography and Data Security*, pages 422–440. Springer, 2016.

[20] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. The emperor's new password manager: Security analysis of web-based password managers. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, pages 465–479, 2014.

[21] Carlos Luevanos, John Elizarraras, Khai Hirschi, and Jyh-haw Yeh. Analysis on the security and use of password managers. In *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pages 17–24. IEEE, 2017.

[22] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. Better managed than memorized? studying the impact of managers on password strength and reuse. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 203–220, 2018.

[23] Peter Mayer, Collins W Munyendo, Michelle L Mazurek, and Adam J Aviv. Why users (don't) use password managers at a large educational institution. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1849–1866, 2022.

[24] Burak Merdenyan and Helen Petrie. Perceptions of risk, benefits and likelihood of undertaking password management behaviours: four components. In *IFIP Conference on Human-Computer Interaction*, pages 549–563. Springer, 2019.

[25] NIST. Digital identity guidelines: Authentication and lifecycle management. 2017. `https://pages.nist.gov/800-63-3/sp800-63b.html`.

[26] NordPass. Password habits in the us and the uk: This is what we found. 2020. `https://nordpass.com/blog/password-habits-statistics/`.

[27] Don Norman. Some observations on mental models. In *Mental Models*, pages 7–14. Psychology Press, 1983.

[28] Sean Oesch and Scott Ruoti. That was then, this is now: A security evaluation of password generation, storage, and autofill in browser-based password managers. In *USENIX Security Symposium*, pages 2165–2182, 2020.

[29] Sean Oesch, Scott Ruoti, James Simmons, and Anuj Gautam. "it basically started using me:" an observational study of password manager usage. In *CHI Conference on Human Factors in Computing Systems*, pages 1–23, 2022.

[30] Chang Sup Park and Barbara K Kaye. Smartphone and self-extension: Functionally, anthropomorphically, and ontologically extending self via the smartphone. *Mobile Media & Communication*, 7(2):215–231, 2019.

[31] PasswordManager. 65 per cent of people don't trust password managers despite 60 per cent experiencing a data breach. 2020. `https://www.passwordmanager.com/password-manager-trust-survey/#:~:text=Despite%20the%20fact%20that%20password,to%2021.5%25%20of%20single%20people`.

[32] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, pages 319–338, 2019.

[33] Zhang Rui and Zheng Yan. A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE access*, 7:5994–6009, 2018.

[34] Marc Schink, Alexander Wagner, Florian Unterstein, and Johann Heyszl. Security and trust in open source security tokens. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 176–201, 2021.

[35] Sunyoung Seiler-Hwang, Patricia Arias-Cabarcos, Andrés Marín, Florina Almenares, Daniel Díaz-Sánchez, and Christian 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*, pages 1937–1953, 2019.

[36] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Transactions on Information and System Security (TISSEC)*, 18(4):1–34, 2016.

[37] David Silver, Suman Jana, Dan Boneh, Eric Chen, and Collin Jackson. Password managers: Attacks and defenses. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, pages 449–464, 2014.

[38] Elizabeth Stobert and Robert Biddle. Memory retrieval and graphical passwords. In *Proceedings of the ninth symposium on usable privacy and security*, pages 1–14, 2013.

[39] Elizabeth Stobert and Robert Biddle. The password life cycle: user behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 243–255, 2014.

[40] Elizabeth Stobert and Robert Biddle. A password manager that doesn't remember passwords. In *Proceedings of the 2014 New Security Paradigms Workshop*, pages 39–52, 2014.

[41] Elizabeth Stobert, Alain Forget, Sonia Chiasson, Paul C Van Oorschot, and Robert Biddle. Exploring usability effects of increasing security in click-based graphical passwords. In *Proceedings of the 26th Annual Computer Security Applications Conference*, pages 79–88, 2010.

[42] Elizabeth Stobert, Tina Safaie, Heather Molyneaux, Mohammad Mannan, and Amr Youssef. Bypass: Reconsidering the usability of password managers. In *International Conference on Security and Privacy in Communication Systems*, pages 446–466. Springer, 2020.

[43] Leona Tam, Myron Glassman, and Mark Vandenwauver. The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 29(3):233–244, 2010.

[44] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do users' perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3748–3760, 2016.

[45] Melanie Volkamer and Karen Renaud. Mental models–general introduction and review of their application to human-centred security. In *Number Theory and Cryptography*, pages 255–280. Springer, 2013.

[46] Chun Wang, Steve TK Jan, Hang Hu, Douglas Bossart, and Gang Wang. The next domino to fall: Empirical analysis of user passwords across online services. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, pages 196–203, 2018.

[47] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, pages 1–16, 2010.

[48] Monica Webster. Nordpass: Overcoming password stress. 2020. `https://nordpass.com/blog/overcoming-password-stress/`.

[49] Leah Zhang-Kennedy, Sonia Chiasson, and Paul van Oorschot. Revisiting password rules: facilitating human management of passwords. In *2016 APWG symposium on electronic crime research (eCrime)*, pages 1–10. IEEE, 2016.

Appendix A

Ethics Approval for Survey Study

Office of Research Ethics
4500 ARISE Building | 1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
613-520-2600 Ext: 2517
ethics@carleton.ca

CERTIFICATION OF INSTITUTIONAL ETHICS CLEARANCE

The following research has been granted clearance by the Carleton University Research Ethics Board-B (CUREB-B). CUREB-B is constituted and operates in compliance with the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS2).

Ethics Clearance ID: Project # 116069

Project Team Members: Sonia Chiasson (Primary Investigator)
Svetlana Dobrynina (Student Researcher)
Elizabeth Stobert (Research Supervisor)

Study Title: Password management habits of Internet users

Funding Source: (If applicable):

Effective: August 05, 2021 **Expires:** August 31, 2022

This certification is subject to the following conditions:

1. Clearance is granted only for the research and purposes described in the application.
2. Any modification to the approved research must be submitted to CUREB-B via a Change to Protocol Form. All changes must be cleared prior to the continuance of the research.
3. An Annual Status Report for the renewal or closure of ethics clearance must be submitted and cleared by the renewal date listed above. Failure to submit the Annual Status Report will result in the closure of the file. If funding is associated, funds will be frozen.
4. During the course of the study, if you encounter an adverse event, material incidental finding, protocol deviation or other unanticipated problem, you must complete and submit a Report of Adverse Events and Unanticipated Problems Form.
5. It is the responsibility of the student to notify their supervisor of any adverse events, changes to their application, or requests to renew/close the protocol.
6. Failure to conduct the research in accordance with the principles of the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans 2nd edition* and the *Carleton University Policies and Procedures for the Ethical Conduct of Research* may result in the suspension or termination of the research project.

IMPORTANT: Special requirements for COVID-19:

If this study involves **in-person research interactions with human participants,** whether on- or off-campus, the following rules apply:

1. Upon receiving clearance from CUREB, please seek the approval of the relevant Dean for your research. Provide a copy of your CUREB clearance to the Dean for their records. See Principles and Procedures for On-campus Research at Carleton University and note that this document applies both to on- and off-campus research that involves human participants. Please contact your Dean's Office for more information about obtaining their approval.

2. Provide a copy of the Dean's approval to the Office of Research Ethics prior to starting any in-person research activities.

3. If the Dean’s approval requires any significant change(s) to any element of the study, you must notify the Office of Research Ethics of such change(s).

Upon reasonable request, it is the policy of CUREB, for cleared protocols, to release the name of the PI, the title of the project, and the date of clearance and any renewal(s).

Please email the Research Compliance Coordinators at ethics@carleton.ca if you have any questions.

CLEARED BY: **Date: August 05, 2021**

BCampbell

Bernadette Campbell, PhD., Chair, CUREB-A

Kathryn Dupré, PhD, Vice-Chair, CUREB-A

Carleton
UNIVERSITY
Canada's Capital University

Informed Consent Form

Project Title: Password management habits of Internet users.
This research has been cleared by Carleton University Research Ethics Board-B (Clearance # 116069).

The purpose of the study. Online users are regularly faced with the need to enter their credentials (usernames and passwords) to access their accounts. Previous research shows that users have different strategies for creating and managing their passwords. This study will explore internet users' habits in managing their passwords as well as their perceptions of special tools designed to securely administer user passwords.

Eligibility. To participate in this study, you must be at least 18 years old and able to respond to a survey in English.

Task. The study involves one online questionnaire, which takes approximately 15 minutes to complete. The questionnaire begins with demographic questions and continues with questions about Internet users' password management habits, experience of using (or not using) some password management tools, and perception of these tools.

Payment. You will be paid £1.88 (approximately 3.26CAD) through Prolific for completing the survey. You will not be paid if you do not complete and submit the survey.

Risks and Inconveniences. The risks associated with your participation in this study are no greater than the risks you take in your daily activities at work or at school. While this risk is expected to be minimal, we will take precautions to protect your identity. Your responses will be confidential but might be disclosed in case of data breach or court order.

Withdrawal. Participation in the survey is completely voluntary and you have the right to end your participation at any time until submitting your responses. To withdraw, close the browser window containing the survey before completing it or return your submission on the Prolific website by selecting the "Stop without completing" button. After you have submitted your responses, you can no longer withdraw from the study.

Data Storage and Protection. Your data will be stored and protected by Qualtrics XM on Canadian servers but may be disclosed via a court order or data breach. After project completion, the data will be retained indefinitely on the lead researcher's password protected computer for the use in thesis and publications. No identifiable information will be collected and Prolific will not disclose participants' personal information to the researcher. Collected data will only be accessible by the research team.

Follow-up interview. At the end of the survey, you will have the option to leave your contact information for a follow-up interview. If interested, you will be asked to provide your Prolific ID. You will only be contacted if you agree to participate. Your choice will in no way affect the payment for completing this survey.
Your Prolific ID will only be used to contact you for the follow-up study. Only researchers directly involved in the research will have access to your Prolific ID. If you participate in a follow-up interview, researchers will be able to link your survey data and your Prolific ID to discuss your responses in more

detail. If you agreed to participate, you can still choose not to be interviewed once contacted by the researcher and your Prolific ID will be destroyed. Prolific ID of those who volunteer to participate in the follow-up interview will be stored separately from the survey data in a password protected file on the lead researcher's computer and will be deleted once the follow-up study is completed. If you do not consent to be contacted for an interview, select "No, I do not wish to be contacted" at the end of the survey.

This project was reviewed and received ethics clearance by the Carleton University Research Ethics Board B (CUREB-B). If you have any ethical concerns with the study, please contact Carleton University Research Ethics Board by email at ethics@carleton.ca.

Researcher's contact information
Svetlana Dobrynina, Human Computer Interaction, Carleton University
Email: svetlanadobrynina@cmail.carleton.ca

Supervisors' contact information:
Prof. Elizabeth Stobert, School of Computer Science, Carleton University
Email: elizabeth.stobert@carleton.ca
Prof. Sonia Chiasson, School of Computer Science, Carleton University
Email: chiasson@scs.carleton.ca

By clicking on "I agree" button at the bottom of this page you give your consent to participate in this survey.

Appendix B

Survey Questionnaire

Carleton
UNIVERSITY
Canada's Capital University

Online survey

Title: Password management habits of Internet users

I. Introductory question

1. Have you ever used a password manager?

- No, I don't know what the password manager is and I've never used it
- No, I've heard about password managers but I've never used them
- Yes, I used a password manager, although I don't use it now
- Yes, I am currently a password manager user
- Other

II. Demographic questions

2. Which country are you currently living in? [dropdown list of countries]

3. How do you identify your gender?

- female
- male
- non-binary
- other
- prefer not to answer

4. What age group do you belong to?

- 18-20
- 21-30
- 31-40
- 41-50
- 51-60
- 61 and older

5. What is the highest degree or level of education you have received so far?

- less than high school degree

- high school certificate or equivalent
- vocational school or apprenticeship
- college diploma
- bachelor's degree
- graduate or professional degree

6. What is your area of expertise? (you can indicate this based on the education or your work experience)

[free text]

7. Which of the following categories best describes your employment status? Select all that apply.

- employed (full or part time)
- not employed
- student
- retired
- other

8. How would you describe your computer skills?

- **Basic skills**: I can turn on and off computer; edit, save and print files; navigate websites; send an email
- **Intermediate skills**: I can recognize and save files in various formats (such as .pdf, .doc, .jpg, .html, etc.); add (and save) attachments to email; complete online forms; download files from Internet; create bookmarks to organize browsed pages; customize software tools
- **Advanced skills**: I can attach and use peripheral devices (scanners, printers, media storage); check file properties to determine memory size; install some software; use the history feature in web browsers; use function keys and keyboard shortcuts; recognize spam
- **Proficient skills**: I have formal computer science background and/or significant working experience in this area

II. Password management habits

9. How many online accounts do you think you have for each of the following categories? Please estimate the number of all your accounts, even if you do not use them often. Please do not include the same account in different categories.

- Email
- Banking/financing/investment/taxes
- Social networks (Facebook, Twitter, Instagram, TikTok, Pinterest, Behance, etc.)

- Forums/messengers/communication tools (e.g., Quora, Slack, WhatsApp, Telegram)
- Online shopping (clothes, food, delivery)
- Online media (newspapers, books, magazines, library)
- Movies/music/entertainment/leisure
- Education/work
- Travel (e.g., airlines, hotels, trains, taxi)
- Utilities/services (e.g., phone bills, electricity, Internet, website hosting)
- Gaming
- Cloud storage
- Health
- Security (antivirus, VPN, password managers)
- Software application and service accounts (e.g., operating system accounts, graphic editor and design accounts, web development accounts, etc.)
- Other

10. How many of these accounts do you think you use regularly (at least once a week)? [free text]

11. How do you currently store your passwords? Rate the following options on the scale from 1 to 5, where 1 is "I don't use this method to store any of my passwords" and 5 is "I use this method for all my passwords".

Rating scale:

1 – I don't use this method to store any of my passwords

2 – I use this method for a small number of my passwords

3 – I use this method for around a half of my passwords

4 – I use this method for most of my passwords

5 – I use this method for all my passwords

- write down on paper/in a notebook
- save passwords in an electronic file (or digital note) on my device
- save a file with my passwords in a cloud service
- send a list of passwords to my email
- remember (use my memory)
- save passwords in a web browser (such as Google Chrome, Firefox, Microsoft Edge, Internet Explorer or any other)

- save passwords in manager provided by operating system (such as Apple Keychain, Samsung Pass, Microsoft Authenticator, or any other)
- use a dedicated password manager, a special tool designed for the secure administration of user passwords (just to name a few - Dashline, Keeper, 1Password, McAfee True Key)

12. Do you currently save some of your passwords in a web browser?

- yes
- no

If the participant answered "yes", questions 13 and 14 are displayed. If they answered "no", they proceed to question 15.

13. Indicate the web browser name, that stores your passwords. If you use several web browsers, choose one you use most often.

- Google Chrome
- Safari
- Firefox
- Samsung Internet
- Edge
- Opera
- Internet Explorer
- Other

14. For the web browsers you use to save your passwords, what other functions of this tool do you currently use?

- auto login to my online accounts so I don't have to copy & paste my credentials
- password generation
- form auto filling, when the service automatically detects and fills out forms with saved names, addresses, and telephone numbers
- auto filling credit card information
- synchronization across devices, i.e., using saved passwords on different devices
- password checkup for strength and data breach exposure
- getting alerts to change passwords
- two-factor (or multi-factor) authentication
- I don't use any of the functions listed above

15. Do you currently use a dedicated password manager? This is a special tool (often in a form of application) designed for the secure administration of user passwords. If you are the user of an operating system-based password manager (such as Apple Keychain, Samsung Pass or any other), please, do NOT indicate it as a dedicated password manager.

- Yes, I am currently using a dedicated password manager
- No, I am not using a dedicated password manager now, but used it before
- No, I have never used any dedicated password managers

If the participant answered "yes", questions 16, 17, and 18 are displayed. If they answered "no", they proceed to question 19.

16. Please indicate the name of the password manager you currently use.

1Password, Avast Password Manager, Bitwaden, Dashlane. Encryptr, Enpass, Intuitive Password, Kaspersky, KeePass, Keeper, LastPass, McAfee True Key, NordPass, Norton Password Manager, Password Safe, Pleasant Password Server, SafeInCloud, other

17. Which password manager plan are you currently subscribed to?

- free plan
- personal paid plan
- family paid plan
- business paid plan provided by employer

18. What features of your password manager do you use?

- saving passwords
- password generation
- browser extension
- auto filling, when the service automatically detects and fills out forms with saved addresses or payment info
- password checkup for strength and data breach exposure
- getting alerts to change passwords
- data breach notifications
- synchronization across devices and platforms
- two-factor (or multi-factor) authentication
- protected credit card storage

- protected file storage
- secure password sharing
- emergency access/emergency contacts
- encrypted messaging
- VPN access
- travel mode
- other
- I don't use any of the functions listed above

III. Mental models of password security and password managers

19. On a scale from 1 to 5, where 1 is "strongly disagree" and 5 is "strongly agree", please rate your agreement with the following statements:

Rating scale: 1 – strongly disagree, 2 – somewhat disagree, 3 – neither agree nor disagree, 4 – somewhat agree, 5 – strongly agree

- I am quite confident that I can manage my passwords securely
- I am satisfied with my approach to manage my passwords
- I find it rather difficult to manage my passwords
- I feel overwhelmed by the need to manage my passwords

20. In your opinion, how secure are the following ways to store passwords? Rate the options on a scale from 1 to 5, where 1 is "not at all secure" and 5 is "the most secure".

Rating scale: 1 – not at all secure, 3 – somewhat secure, 5 – the most secure

- write or print passwords and store a piece of paper (or notebook) in a secure place at home
- write or print passwords and keep a piece of paper (or notebook) on my laptop/desk always at hand when I need it
- remember (use memory)
- keep an electronic file on my personal device protected with a password
- keep an electronic file on my personal device without password protection
- have digital notes on my personal smartphone or tablet
- save a file with passwords in cloud service
- send a list of passwords to my email
- save passwords in web browsers
- save passwords in dedicated password managers

- save passwords in operating system (e.g., Apple Keychain on iOS devices; Microsoft Authenticator phone app on Microsoft Windows devices)

21. In your opinion, how convenient are the following ways to store passwords? Rate the options on a scale from 1 to 5, where 1 is "not at all convenient" and 5 is "the most convenient".

Rating scale: 1 – not at all convenient, 3 – somewhat convenient, 5 – the most convenient

- the same list as in Q20.

22. Do you have passwords that you don't save in either your web browser or a dedicated password manager?

- yes
- no

If the participant answered "yes", question is 23 displayed. If they answered "no", they proceed to question 24.

23. For passwords that you chose not to save in a web browser or a dedicated password manager, please, indicate the reasons for not using these tools? Please choose up to three of the most applicable options.

- I don't think my passwords are of interest to anyone so I don't think I need to use these tools
- I don't have a problem of storing my passwords in other ways
- I am afraid of sharing my passwords externally and prefer to keep them locally with me
- I didn't know about existing of these tools
- I don't trust these tools as I'm not sure how they work
- I don't trust these tools as companies can steal my data
- I can't decide which browser or password manager application to choose
- I don't know how to use these tools
- I think I have some technical issues with my device(s) (i.e., insufficient memory space, the device is slow, the battery is consumed quickly)
- other people have access to my device, so I don't want my passwords to be accidentally disclosed to them
- I don't trust my devices (i.e., my device can be hacked or stolen and the passwords will be compromised)
- other

24. [the question is displayed to those participants who answered yes to Q12] **Why do you save some of your passwords in a web browser? Please choose up to three of the most applicable options.**

- I do not have to remember my usernames and passwords for some of my accounts
- I do not have to fill in the login fields manually every time

- I can automatically login to my accounts across all my devices (i.e., synchronization function)
- web browser auto-fills the online forms for me (i.e., it remembers my address, name, telephone number)
- it provides some other useful features (e.g., two-factor authentication, password generation, password change alerts)
- it enhances the security of my passwords as the browser stores them encrypted
- I can use stronger passwords for my accounts as the tool remembers them for me
- someone I trust suggested me to use it, so I just believe them
- it's an automatic function of my browser so I don't know how to turn it off or to delete my previously saved passwords
- other

25. [the question is displayed to those participants who answered no to Q15] **Why don't you currently use a dedicated password manager to store your passwords? Please choose up to 3 answers that best describe your reasons.**

- I don't think my passwords are of interest to anyone, so I don't think I need a dedicated password manager
- I don't have a problem of storing my passwords in other ways
- I haven't heard of this tool before participating in this survey
- I don't trust these tools as I'm not sure how they work
- I don't know how to use these tools
- I don't trust these tools as companies can steal and use my data
- I probably would like to start using it, but I can't decide which password manager to choose
- choosing, installing, and transition to it requires extra efforts from me, so I don't have enough time and motivation to do it
- I am afraid of losing my master password
- I think I have some technical issues with my device(s) (i.e., insufficient memory space, the device is slow, the battery is consumed quickly)
- I don't trust my devices (i.e., my device can be hacked and the passwords will be compromised)
- other people have access to my device, so I don't want my passwords to be accidentally disclosed to them
- other

26. [the question is displayed to those participants who answered "yes" to Q15] **Why do you use a dedicated password manager to store your passwords? Please choose up to 3 answers that best describe your reasons.**

- It is convenient to save usernames and passwords for some of my accounts
- I don't have to fill in the login fields manually every time
- I can automatically login to my accounts across my devices (i.e., synchronization function)
- web browser extension auto-fills the online forms for me (i.e., it remembers my address, name, telephone number)
- it provides some other useful features (e.g., two-factor authentication, password generation, password change alerts)
- it enhances the security of my passwords as the manager stores them encrypted
- I can use stronger passwords for my accounts as the tool remembers them for me
- someone I trust suggested/subscribed me to use it, so I just believe them
- it was included in my antivirus package, so I just follow the recommendations of the antivirus company
- my employer provided access to the password manager, so I use it to manage both my work and personal accounts
- other

27. On a scale of 1 to 5, where 1 is "strongly disagree" and 5 is "strongly agree", rate how agree you are that the following statements are true.

Rating scale: 1 – strongly disagree, 2 – somewhat disagree, 3 – neither agree nor disagree, 4 – somewhat agree, 5 – strongly agree

A web browser that stores its users' passwords…

- gives extra protection for user passwords and usernames
- offers more usable and convenient way to manage user passwords
- takes time to learn how to use it
- takes time to transfer passwords to it
- may disclose users' passwords to third parties
- its employees can have access to user data
- puts user data at greater risk

A dedicated password manager that stores its users' passwords…

- gives extra protection for user passwords and usernames
- offers more usable and convenient way to manage user passwords

- takes time to learn how to use it
- takes time to transfer passwords to it
- may disclose users' passwords to third parties
- its employees can have access to user data
- puts user data at greater risk

IV. Follow-up interview

28. Would you like to get contacted for a potential follow-up interview? If you agree to be contacted about the interview, you will be asked to provide your Prolific ID for sending you study information. Your decision will not impact your payment for the current survey. The participation in the interview is also paid.

- Yes, please contact me for a potential follow-up interview. My Prolific ID is ________
- No, I do not wish to be contacted

Appendix C

Ethics Approval for Interview Study

Office of Research Ethics
4500 ARISE Building | 1125 Colonel By Drive
Ottawa, Ontario K1S 5B6
613-520-2600 Ext: 4085
ethics@carleton.ca

CERTIFICATION OF INSTITUTIONAL ETHICS CLEARANCE

The following research has been granted clearance by the Carleton University Research Ethics Board-B (CUREB-B). CUREB-B is constituted and operates in compliance with the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS2).

Ethics Clearance ID: Project # 116363

Project Team Members: Sonia Chiasson (Primary Investigator)
Svetlana Dobrynina (Student - MA student)
Elizabeth Stobert (Research Supervisor)

Study Title: Password management habits of Internet users

Funding Source: (If applicable):

Awards File No	Title	Status	
111747	Cognition-Informed Security	Active	A. OVPRI Approval Form

Effective: October 21, 2021 **Expires:** October 31, 2022

This certification is subject to the following conditions:

1. Clearance is granted only for the research and purposes described in the application.
2. Any modification to the approved research must be submitted to CUREB-B via a Change to Protocol Form. All changes must be cleared prior to the continuance of the research.
3. An Annual Status Report for the renewal or closure of ethics clearance must be submitted and cleared by the renewal date listed above. Failure to submit the Annual Status Report will result in the closure of the file. If funding is associated, funds will be frozen.
4. During the course of the study, if you encounter an adverse event, material incidental finding, protocol deviation or other unanticipated problem, you must complete and submit a Report of Adverse Events and Unanticipated Problems Form.
5. It is the responsibility of the student to notify their supervisor of any adverse events, changes to their application, or requests to renew/close the protocol.
6. Failure to conduct the research in accordance with the principles of the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans 2nd edition* and the *Carleton University Policies and Procedures for the Ethical Conduct of Research* may result in the suspension or termination of the research project.

IMPORTANT: Special requirements for COVID-19:

If this study involves **in-person research interactions with human participants,** whether on- or off-campus, the following rules apply:

1. Upon receiving clearance from CUREB, please seek the approval of the relevant Dean for your research. Provide a copy of your CUREB clearance to the Dean for their records. See Principles and Procedures for On-campus Research at Carleton University and note that this document applies both to on- and off-campus research that involves human participants. Please contact your Dean's Office for more information about obtaining their approval.
2. Provide a copy of the Dean's approval to the Office of Research Ethics prior to starting any in-person research activities.
3. If the Dean’s approval requires any significant change(s) to any element of the study, you must notify the Office of Research Ethics of such change(s).

Upon reasonable request, it is the policy of CUREB, for cleared protocols, to release the name of the PI, the title of the project, and the date of clearance and any renewal(s).

Please email the Research Compliance Coordinators at ethics@carleton.ca if you have any questions.

CLEARED BY: **Date: October 21, 2021**

BCampbell

Bernadette Campbell, PhD, Chair, CUREB-B

KEDupré

Kathryne Dupre, PhD, Co-Chair, CUREB-B

Informed Consent Form

Project Title: Password management habits of Internet users.
This research has been cleared by Carleton University Research Ethics Board-B (Clearance #116363).

The purpose of the study. Online users regularly enter their credentials (usernames and passwords) to access their accounts. Previous research shows that users have different strategies for creating and managing their passwords. This study will explore Internet users' habits in managing their passwords as well as their perceptions of special tools designed to securely administer user accounts.

Eligibility. To participate in this study, you must be at least 18 years old and able to communicate in English.

Task. The study involves a one-on-one online interview via Zoom (https://zoom.us/), which takes approximately 40 minutes. During the interview, we will ask about your password management strategies and perceptions of special tools for secure password management. To enable us to accurately capture your comments, we will audio record the Zoom session, no one outside of the research team will hear the audio recordings. During the session, you may turn off your video camera. If you do not wish to be audio-recorded, then you cannot participate in this study.

If you do not consent to be contacted for an interview, select "No, I do not wish to be contacted" at the end of this form.

Payment. You will be paid 15 CAD through e-transfer for participating in the interview.

Risks and Inconveniences. The risks associated with your participation in this study are no greater than the risks you take in your daily activities at work or at school. While this risk is expected to be minimal, we will take precautions to protect your identity. Your responses will be confidential but might be disclosed in case of data breach or court order.

Withdrawal. Participation in the interview is completely voluntary and you have the right to end your participation at any point before and during the session simply by informing the researcher. If you withdraw, the researcher will ask whether the information collected from you before your withdrawal can still be used or whether it should be removed from the study data. If you wish your data to be removed, it will be immediately destroyed. If you change your mind after the interview, you have 72 hours after the session to withdraw your interview data by emailing the researcher. If you withdraw after the session, you may keep the full compensation.

Data Storage and Protection. Your Consent Form data will be stored and protected by Qualtrics XM on Canadian servers but may be disclosed via a court order or data breach. All interviews will be conducted and audio-recorded via the Zoom platform and written notes will be taken by the researcher. You do not need to have a registered account to access a Zoom meeting, so you can remain anonymous to the service. Zoom operates through its data center in Toronto, Canada, and allows its customers to comply with Canadian privacy laws. Audio recorded data will be saved directly on the researcher's local drive and will be kept in a password protected folder.
The researcher will use Trint, an online software, to transcribe audio recordings. The files will be deleted from the researcher's Trint account after the completion of the data transcribing process and will be

kept in a password protected folder on the researcher's local drive. Trint has servers located in the United States, therefore, the data may be subject to the US laws on data privacy.

After project completion, the anonymized data will be retained indefinitely on the lead researcher's password protected computer for the use in thesis and publications. Your email address will be deleted 72 hours after the interview, once the withdrawal period has expired. No other identifiable information will be collected. Collected data will only be accessible by the research team.

This project was reviewed and received ethics clearance by the Carleton University Research Ethics Board B (CUREB-B). If you have any ethical concerns with the study, please contact Carleton University Research Ethics Board by email at ethics@carleton.ca.

Researcher's contact information
Svetlana Dobrynina, Human Computer Interaction, Carleton University
Email: svetlanadobrynina@cmail.carleton.ca

Supervisors' contact information:
Prof. Elizabeth Stobert, School of Computer Science, Carleton University
Email: elizabeth.stobert@carleton.ca
Prof. Sonia Chiasson, School of Computer Science, Carleton University
Email: chiasson@scs.carleton.ca

put your name here

I voluntarily agree to participate in this study and I agree to be audio recorded (If you do not agree to be audio-recorded, you will not be able to participate in the study. We need the audio recording to ensure that we accurately capture your feedback).

put your name here

No, I do not wish to participate in this study

Appendix D

Interview Guide

Carleton
UNIVERSITY
Canada's Capital University

Interview questions

(with notes for researcher highlighted in *blue*)

The following are sample questions for a semi-structured interview. We may deviate slightly depending on participant answers, but these are the general topics to be discussed. At no point will we ask for information about participants' actual passwords.

Introduction: Hello, my name is Sveta, I am the lead researcher of the project. The project explores Internet users' habits in managing their passwords and their perceptions of special tools designed to securely administer user accounts.

There are no right or wrong answers: everything you say helps us learn more about how real people manage their accounts and perceive the various tools that can help them keep track of their passwords. We encourage you to be open about your experiences and thoughts. I will not ask you to disclose your passwords or any personal identifiable information during this interview.

If you feel uncomfortable answering any question, let me know and we can skip that particular question. You can end the interview at any time during our session without giving any explanation.

Do you have any questions before we begin?

Now I'm going to start audio recording. Please turn off your video camera so that we only capture audio.

1. How do users' password management habits and strategies differ between our three user groups?

- What kinds of strategies do you use to handle passwords? *Possible clarifying question*: How do you store your passwords? What influences your choice of strategies?
- What types of your accounts do you categorize as most important?
  - How do you decide what accounts are important and which are less important?
  - What factors influence your decision?
- How do you manage your important and unimportant accounts?
- Have you ever re-considered the importance of an account? Why did this happen?
- How do your password management strategies differ between your existing accounts and new accounts? If you needed to create a new account, how would you handle it?
- Have you ever changed the way you store passwords? What prompted you to change your approach?

2. How do perceptions and attitudes towards password managers differ between our three user groups?

Next, I will ask you some questions about your perceptions and experiences with password managers. I want to make sure that we are talking about the same thing. Password managers are digital tools to help user store, manage, and sometimes generate passwords.

For example, if a user saves their passwords in a web browser (like within Google Chrome), they are users of a browser based PM. Other PMs are standalone applications (like LastPass), some are built-in to your computer's operating system (like Apple Keychain), and others are included as part of an

antivirus package. Do you have any questions about this? Do you know which of these, if any, you've used before?

Now we will talk about password managers.

- How do you feel about password managers? Who should use them?
- How does a PM work?
    - Where is user data stored?
    - Who has access to user data?
    - How do password managers help with user passwords?
- Can you tell me about your experience with password managers?
- What do you like and dislike about the PM you currently use?
- Do you have any concerns regarding password managers?

3. What factors influenced users of each group in adopting their current approach to password management?

Why?

- Why do you currently use this PM? Why did you start using it?
    - Or: Why don't you currently use a PM?
    - Or: If you used a PM before, why did you stop using it?
- What led you to store your passwords in this way?

How?

- How did you choose this particular PM? Have you ever switched from one PM to another? Why?
- What might influence you to start (or keep) using a PM in the future?
- What might prompt you stop using this PM?

4. How do the perceived pain points from using password managers differ between the three user groups?

- Can you tell me about any negative experiences you've had with password managers?
    - Or: Do you anticipate any negative experiences with the password managers?
- Have you faced any challenges with password managers? How did you deal with these?
    - Or: Do you anticipate any challenges with password managers?
- Is there anything that might discourage you from using a password manager?

Closing question

Did I miss anything? Is there anything else you'd like to share about your opinion or your experience with password management and password managers?

What do you consider to be the most important points from our discussion that I should note?