Factors Affecting Password Manager Adoption among European University Students

UNIVERSITY OF TURKU
Department of Future Technologies
Master of Science in Technology Thesis
Security of Networked Systems
November 2019
Alina Dubinina

Supervisors:
Ali Farooq, MSc.
Antti Hakkala, PhD(Tech.)

UNIVERSITY OF TURKU
Department of Future Technologies

ALINA DUBININA: Factors Affecting Password Manager Adoption among European University Students

Master of Science in Technology Thesis, 59 p., 6 app. p.
Networked Systems Security
November 2019

Password is the most common method of proving the identity on various online services. More and more sensitive information gets stored online: banking details, healthcare data, educational and corporate data. Due to the increasing amount of accounts, users face the challenge of creating and remembering various passwords of high complexity. To deal with such challenges and improve password management practices, security professionals suggest the use of password managers, also known as password managers. However, this tool has not gained much popularity among the end-users.

The purpose of this thesis is to identify and examine the factors that may affect the adoption of password managers. In this regard, I have proposed a research model based on the Unified Theory of Acceptance and Use of Technology (UTAUT) and Task Technology Fit (TTF) models. Data (N=265) was collected from students enrolled at one of European universities using a online survey. For this purpose, data was collected using mailing lists and Facebook page of a crowdsourcing site. PLS-SEM was used to test the proposed model with a usable data set of N= 265.analyze the data sample collected with the means of a questionnaire.

The results of the analysis show that performance expectancy and social influence affect behavioral intentions. Task technology fit, facilitating conditions, and behavioral intentions directly affect password manager adoptions, while performance expectancy, social influence, effort expectancy, and technology characteristics are the main factors that affect password manager adoption among European students indirectly.

Keywords: password managers, password vaults, technology adoption, UTAUT, TTF

Contents

Abbreviations and Acronyms

BI	Behavioural Intentions
CI	Continuance Intentions
EE	Effort Expectancy
FC	Facilitating Conditions
PE	Performance Expectancy
SI	Social Influence
TAM	Technology Acceptance Model
TaskC	Task Characteristics
TC	Task Characteristic
TTF	Task Technology Fit

List of Figures

List of Tables

1 Introduction

1.1 Problem Overview

Internet is an essential part of the modern society lifestyle. More and more previously analog services nowadays move to the Internet, such as television, radio, mail and phone communication. With the increasing amount of opportunities provided by the online services, the number of people that try to exploit those opportunities maliciously grew as well. Performed cyberattacks became more difficult to prevent; they have become much more advanced. The concern is that with the increased number of online services, people started sharing their personal data across the internet. Without proper security measures, the information about health, banking details, private conversations can be exposed or stolen by cybercriminals. This means that if a personal account is hacked – the data loss may affect the user significantly. To protect personal information online, various means of authentication are provided to the users. Authentication is a method of proving a user identity, and it assures that the person is entitled to have access to the data. There are three main ways to authenticate: knowledge-based authentication by using a secret string communicated between the end-user and the system, which is commonly known as password; physical token authentication, and biometric authentication (Brostoff and Sasse, 2000).

Passwords are a very common mean of authentication when accessing a particular web resource or a computer (Maclean and Ophoff, 2019). They are used to protect our sensitive data, such as our health data, our corporate information, banking details, and personal communication. Despite being the most used method of authentication, knowledge-based authentication has quite many flaws. The main one is human memory and its limited capacity. Only around seven chunks of data can be memorized, according to the study by Miller (1956), and there is a high risk to forget some information due to the increasing number of passwords people use. The common rules for creating a secure password are combining various types of characters: upper-case letters, lower-case letters, digits and special characters (Schougaard and Dragoni, 2016). Moreover, a complex password should be at least eight characters long, and it should not contain any known word. The number of different accounts and the complexity of passwords required by security recommendations make it challenging to remember the

passwords (Charoen, Raman, & Olfamn, 2008). Hence many users end up reusing the secret for different resources or write the passwords down on paper, which is a serious security risk. Moreover, there are different attacks targeted towards password authentication nowadays, such as phishing or credential theft (Li and Evans, 2017), so it is important to be aware of the necessary security measures that can prevent the loss of sensitive data. One of the most serious challenges is protecting against the Man-in-the-Browser attack and keylogging since the procedure of logging into the account involves typing the password and the username in the browser window (Golrang, 2012). Keylogger is an application that tracks and detects the sequence of the keystrokes captured from the physical keyboard used to input the password. Some systems have a virtual keyboard available on the web portal, which appears in the different parts of the display, so the keystrokes can never be traced. However, in this case, it is easier for a criminal to look over the shoulder of the user and memorize the password. Moreover, some applications take snapshots of the screen after every mouse click of the user; such applications are called 'screen grabbers' (Golrang, 2012). The Man-in-the-Browser (MIBT) attack has gained its popularity due to the wide usage of the browsers for performing banking operations and using personal e-mail and social media accounts. The MITB attack method combines keystroke capturing, taking screenshots, and stealing credentials. It is quite challenging to protect from this type of attack due to its complexity.

To facilitate the management of passwords, password managers were introduced. Password management software or password managers allow users to delegate generating and storing the passwords securely to the technological devices. There are multiple different password managers available on the market, and they can be divided into four major groups: desktop password manager, online and portable password managers (Karole et al, 2011). The first category of password managers includes those applications that allow the user to keep the passwords on the local machine. An online password manager is installed on the third-party server available across the network. The third category of password managers include the vaults that are installed on the portable device, such as USB flash drives or phones. Access to the database with credentials is protected by a master password, which needs to be memorized. Having to

remember only one password reduces the load on the user's memory since it is only necessary to remember one complex password instead of various. Despite being described as a secure method to manage the credentials, there are still quite a lot of people who choose not to use the software for various reasons (Aurigemma et al, 2017).

1.2 Study Purpose and Research Questions

The purpose of this thesis is to identify the factors that affect the adoption of password management among students in Europe. It is important because using weak passwords or reusing the passwords for multiple accounts poses a threat to the user's sensitive data. Potential attackers can obtain data of the users by hacking their passwords. This study aims at understanding the decision-making behind the adoption of the password managers among the students. The following research questions are intended to be answered in this study:

1. What is a demographic profile of a European student who (does not) use a password manager?
2. What factors affect password manager adoption among the European students?

1.3 Research Methodology and Scope of Study

In order to answer the research questions, quantitative research was conducted. SmartPLS was used for the data analysis. Students are chosen as the target group of this research because they are the future potential employees. The increasing number of passwords used in daily working life makes it critical for companies to make sure their workers use secure methods for managing important work-related credentials. Moreover, the universities have a lot of internally available data such as research and personal data of students and poor password management may lead to security breaches at the universities as well. Password managers are one way of facilitating the use of secure passwords, thus improving the security of the systems.

1.4 Thesis Structure

The rest of the thesis is organized as follows: first, the background information on password managers is given in Chapter 2, including the types of password managers. The existing studies regarding usability and security, as well as user studies conducted regarding the adoption of password vaults will be discussed in detail in order to analyze the current gap in the research. Further, the methodology is presented in Chapter 3.

Various theoretical models used for the thesis research are described along with similar studies done in the past regarding technology adoption. A theoretical model chosen for the research is presented, followed by the hypotheses based on it. Finally, the results of the quantitative research are analyzed in Chapter 4 in order to confirm or deny the hypotheses and answer the research questions.

2 Background

2.1 Password manager definition

Password managers are a tool for storing and organizing passwords so that the users do not have to remember all the credentials they use for different accounts. Password managers also provide the functionality of creating passwords. The software that keeps all the user's login information in a database, and provides the credentials whenever needed (Karole et al, 2011). The passwords are usually encrypted inside the database in order to enhance the level of security. There are several major types of password managers, but they typically share the same features: the password vault is protected by a master key, and if the user wants to access the credentials, it would be necessary to input the key to the software.

2.2 Types of password managers

Password managers were created to provide a tool for storing and managing passwords so that the users do not have to remember all the credentials they use for different accounts. Table 1 summarizes the types of password managers along with examples.

Table 1. Types of password managers

Type of password manager	Vault database location	Examples	Source
Browser-based	Locally inside the browser	Firefox or Chrome browser extensions	Bojan, 2017 Karole et al, 2011
Stand-alone	Locally on the PC as a separate application	1Password, Keepass	
Cloud-based	Remotely on a third-party server	Dashlane, 1Password, LastPass	
Portable	On a USB stick or mobile phone	Keepass, Lazlock, Password Safe	

History of password managers started with the software implemented in the browsers. There are two types of browser-based password managers nowadays: browser-embedded password vaults and browser plugins. Browser-embedded password managers have a password management feature implemented into a browser, such as Internet Explorer, Mozilla Firefox, Google Chrome, and others. The credentials are stored on the local PC of the user and are accessible on-demand. It is possible to have the credentials encrypted by using a master password. However, not all of the browsers use the encryption or a password for protecting the credentials. The browser plugins are

extensions that are installed into the browsers. Popular password managers, such as KeePass, Lastpass and 1Password can be installed into the browser. These password vaults encrypt the credentials database by using the master password provided by the user (Karole et al, 2011). It is possible to use password managers not only for managing passwords but also for storing bank credentials, credit card information and other sensitive data that requires protection. The browser-based password managers have a feature of distributing password database among the all the devices of the user, so it is easier to log in from different locations, nonetheless, it is necessary to be authenticated in the browser in order to be able to synchronize the passwords (Bojan, 2017).

Further, password managers developed, and nowadays there are many different solutions available for the users on the market. Bojan (2017) categorizes the password managers into three major categories: browser-based password managers, stand-alone password managers and cloud-based password vaults. Password managers can also be categorized by the type of the device they are installed on. Karole et al (2011) classifies password managers into the following categories: desktop password managers, portable managers and online password managers Fukumitsu et al (2016) divides password managers into groups as follows: web-browser plugin, a mobile phone application or a web-based software. When password vaults only started to gain their popularity, they were only storing the credentials on one device, which limited the portability of such software. With the increasing need to log into systems from different locations, it was necessary to revise the password management practices, so some applications started offering to store the database on a remote server accessible from different locations or installing a portable password manager to a USB drive or a phone. Mobile password vaults are installed in a form of an application with a password database that is stored locally on a smartphone and can be accessible on-demand.

The stand-alone password managers evolved from the browser-based vaults as an attempt to provide a more secure way of managing the credentials (Bojan,2017). The data in such vaults is encrypted. Stand-by password managers have a number of features besides storing the passwords in the database. Some of the password vaults allow the users to use the credentials generated by the software in compliance with the requested

password requirements. Moreover, password managers are able to check whether the passwords are secure enough. Some software allows sharing the credentials among different password managers and devices, and finally the password managers are able to analyse the security of the websites used by the individual and can prompt to change the password on some web portal if the site is not considered secure or if it had suffered a security breach (Bojan, 2017). Finally, cloud-based password managers provide the user with the possibility to access the password database from anywhere. It is only necessary for the individual to have access to internet and to the web browser in order to log into the cloud and start using the credentials. Moreover, the cloud provider is assuring the reliability of the servers: the data is usually backed up, so in case of the failure of the storage or the server, the user can easily recover the credentials and continue using the services without problems. The drawback of the online password manager is that the user has to trust the service provider with the credentials, and some online password management services do not provide the client with enough information on how their data is being secured (Karole et al, 2011).

2.3 Features and Limitations of Password Managers

Prior to the investigation on the adoption of password managers among students, a systematic literature review has been completed. The difference from a regular literature review is that during the systematic literature review all the relevant publication and research is collected. Any mention of the subject in the published and unpublished studies makes an article or a book a subject of investigation in terms of relevance. The systematic literature review provides a more detailed view on the subject, and since all research is being identified, it reduces the possibility of bias (Nightingale, 2009).

There are several steps necessary to be taken in order to conduct a proper literature review: first, the goal is being determined. One has to define what the objective of the study is, and what the main subject of the research is going to be in order to define the search keywords later. The second step is to decide the criteria that will serve as a basis for deciding whether the study will be considered as relevant. Next step is to decide on the manner in which the research is going to be identified, and then the analysis strategy is done as a final step of the systematic literature review (Nightingale, 2009). It is important to identify all the possible studies that were covering the subject of interest.

This way not only the well-known publications that reached important journals will be analyzed but also the articles that got less publicity. After the publications have been identified, it is necessary to go through the array of the articles or chapters found in different databases and remove the duplicates found. It is possible that one will need to do a search various times before collecting all the possible relevant studies. Next, the first screening is done, by analyzing the abstract and the title of the research, as well as its type. At this stage, some articles may be removed as irrelevant or not suitable for a scientific study, such as websites. After, it is necessary to go through the articles in-depth and decide whether each of the publications should be kept as relevant or excluded with reasoning.

A search string was created and adapted for different major scientific databases, and each of them was searched against the string. The search was done in two phases, since during the first phase it was identified that there are various synonyms for the term ‘password manager’, such as ‘password vault’ and ‘password keeper’. Hence, the search string for the second phase of the literature review had to be modified. During the first phase, a total of 202 articles were found in six major scientific databases: Scopus, Web of Science, Google Scholar, IEEE, Science Direct and ACM. 65 duplicate entries were found and removed. During phase two, 26 articles were found, of which 9 were removed as duplicated. The next step in the systematic literature review was to identify the relevant studies. First, they were identified solely by the titles, then by the contents. A total of 62 publications were marked as relevant. It was important to go through the studies one more time and identify the main categories of publications. This step simplifies the further analysis of the literature and the shortcomings in the currently available research. The collected articles were later classified by the categories by major topics: design of password managers, usability studies, user-related studies, guidelines for using studies, articles related to types of password managers, review papers, and the unclassified studies, which include the studies that cover two or more different topics related to password vaults.

Systematic literature review shows that there are two most popular features of password managers studied previously: usability and security. Nowadays password vaults include

several important features that are intended to provide the user with a secure and pleasant experience. Despite providing a user with useful features for convenient and secure password management, different types of password vaults have certain limitations. There are concerns about the protection of the sensitive data ensured by the password manager provider and the operating system of the mobile device in case of portable password vaults. Furthermore, consumers are concerned by the fact that the application might be sharing sensitive data with the third-party, which might collect sensitive information about the users. The mobile password managers do not often provide the users with any additional features besides storing usernames and passwords, so the user cannot store the credit card data or banking information. Finally, the embedded password managers do not allow the user to switch between devices, so if the individual was to log into a system from another smartphone, there is no possibility to access the password database. An online vault is accessible from different workstations if the network access is configured. However, use of it requires the trust of the user to outsource the storage of the passwords to a third-party server. The transparency and security are not always guaranteed by the service provider. Moreover, the encrypted password is transmitted across the public network, which poses a risk of the traffic being captured by a hacker. It is possible to decrypt the passwords by using a brute-force attack because the master password might be poorly created. Furthermore, a malicious entity can gain access to multiple databases of passwords in case the server is hacked. Even though the credentials are encrypted, it is not guaranteed that they will not get decrypted. Portable password managers seem more trusted since the user has full control over the management of the portable device where the passwords are stored. Nevertheless, mobile vaults do not allow copying the passwords directly into the password text field, so the user must manually input the credentials. This results in a lack of usability. USB portable managers help avoid the necessity of typing the passwords manually, however, the users might not always have USB accessible as easily as a mobile phone (Karole et al, 2011).

Human memory capacity is limited; therefore, it is complicated to follow the guidelines of creating long and complicated diverse passwords. The general principle of browser-based password manager operation is described as follows: each time the individual

creates an entry about a new webpage into the software, it is necessary to input the link of the website, the username, and the password (Fukumitsu et al, 2016). The information entered by the user is further encrypted. The database is encrypted with the use of the master password that the user has to create. Browser-based password managers automatically inject the credentials one the individual visits the page that is included in the database. Master password, in this case, it becomes the single point of failure, which compromises the security of the software. The mitigation strategy suggested by Fukumitsu et al (2016) is to use a method of two-factor authentication: a security token. Since the master password is created by a human, it might not comply with the security guidelines and compromise the integrity and confidentiality of the password manager database. Hence, a token may provide an additional level of security. However, the token is not protected against the human error: people tend to leave the token at convenient places near the PC, which allows the potential attacker to take ownership over the token and hack the password database (Fukumitsu et al, 2016).

Several password vault prototypes have been suggested by researchers that were aimed at offering various solutions in terms of usability and security, as well as functionality. The proposal by McCarney et al (2012) suggests that the mobile phone can be used as a security token, and an additional asset in order to separate the key used to decrypt the data and the encrypted database. The main shortcoming of the proposed model is that in case the smartphone is lost, it is not possible to recover the data. Fukumitsu et al (2016) raise concerns about the security and usability of password managers. The suggestion described by Fukumitsu et al (2016) is to enhance the model by McCarney et al (2012). The scheme involves a personally assigned server, a user's PC and a smartphone. First, it is important to set up secure communication such as TLS in order not to send plain text data between the devices. Second, the user is required to create a strong enough server password. Even though there is a human error involved, the fact that the server is only a part of the whole schema reduces the risk of the data loss if the user discloses the password or makes it too easy to hack. The password manager design was further revised against the UDS model: usability, deployability, and security (Bonneau et al, 2012). In terms of usability, the proposed model has an easy way to recover the data in case the smartphone is lost, or the server password is forgotten. The deployability is

imperfect due to the fact that it is quite expensive since it requires the installations of three devices. Furthermore, it is necessary to configure the browser to meet the requirements for the installation of the password manager proposed in the study (Fukumitsu et al, 2016). Finally, the security advantages are quite strong, because there are three parties involved, so it makes it more difficult for the attacker to hack the passwords. The shortcoming of this password manager is the deployability of it. There should be improvements done on the way the password manager is installed and configured.

Stobert and Biddle (2014) discuss different password management techniques in detail. They mention graphical passwords, which could be a good alternative solution to the problem of password management. The study claims that using pictures instead of character sequence is better due to the fact that humans are better at remembering graphical information than text. The adoption of a graphical password is not wide, however, there is a potential for them to get more popular throughout the years. There are various implementations of such authentication method, for example, a dot sequence on Android devices for unlocking the screen. Windows also provides the users with an opportunity to sign in using a picture. There are however drawbacks when using a graphical password. there are certain areas which the users are more likely to be selected as a part of the pattern. The workaround for this problem is using a pattern created randomly. The paper suggests a cued graphical password. The idea is to provide the user with a memorable clue in order to recall the credentials. One of the variations of the cues is the secret questions that normally serve as help for the users to reset the password. An example of a graphical password manager mentioned by Stobert and Biddle (2014), is PassTiles. The software allows the user to log into the system by clicking a sequence of tiles in a grid. When the individual creates the password, the tiles get charted, so that the sequence can be remembered. The user chooses the tiles on the basis of a picture; however, the image is always different and randomly generated. The proposed design can help avoid the phishing attack due to the fact that it is complicated for the hacker to obtain the information about the password when it is graphics-based.

2.4 Security Issues of Password Managers

The security of password managers is the main feature of password vaults. It is important to provide the users with the features that will protect their sensitive data from being stolen or compromised. Li and Evans (2017) classify the vulnerabilities of password managers into two main categories: client-side and server-side. Client-side vulnerabilities are network-related or user-related, while server-side affect the password vault itself whereas server vulnerabilities affect the password database. The authors of the aforementioned article state that there are four goals that the password managers need to pursue as a software in order to remain secure. First of all, it is crucial for a password vault to protect the account's security. Furthermore, the credentials database has to stay secured. The accounts of collaborators have to keep their integrity. Finally, there should not be any possibility for the credentials' leak, such as applications intercepting and capturing the credentials.

2.4.1 Function-Specific Vulnerabilities

Several functions of password managers were discovered to be vulnerable to various exploits. Li and Evans (2017) open a discussion about the security of password managers in practice. The research is aiming at identifying the risks associated with the use of password managers, especially poorly secured ones, as well as highlighting the guidelines on how to use the vaults properly in order to benefit from them. Security of the software is studied in-depth: there were several attacks performed in order to investigate the possible vulnerabilities and find out how severe the risks of using password managers can be. The features of the password managers that were being studied include encryption on the client-side, a possibility of autofill and having single-use passwords (Li and Evans, 2017). The study mentions the autofill vulnerabilities and the fact that it is possible to obtain the credentials by using a script. Javascript functions can be exploited, and password managers lack the functionality of detecting the legitimacy of the scripts, hence there is a risk of the data loss. Moreover, Li and Evans (2017) claim that there may be bugs in the client scripts, that exposed the users to the attacks. The hacker could exploit LastPass and obtain user credentials through a non-legitimate domain URL because the password manager did not correctly recognize the domain from the URL.

Further into the investigation, in order to research the security of password managers in-depth, Li and Evans (2017) focus on four main vulnerabilities of the applications: the user interface vulnerability, authorization vulnerability, web and bookmarklet vulnerabilities. The user interface vulnerabilities involve phishing: if the password gets stolen during the phishing attack, it can compromise the confidentiality and integrity of the entire password database. Bookmarklets were studied, and vulnerabilities were discovered in all the showcases mentioned in the article. The attacker can create a malicious page, and in case the individual uses this feature for logging in on such a page, the hacker gets an opportunity to steal the credentials. XSS and CSRF are the common vulnerabilities that affect password managers. Regarding the authorization vulnerability, it is related to the feature of collaboration provided by some of the password vaults. Some password vaults, such as My1login, give an opportunity of granting certain permissions for different users so that there is a better control over the access to credentials. Authorization allows a more granular control yet a possibility for several users to collaborate in terms of managing passwords. The software might provide the excessive authorization rights to a user that is not supposed to have them. With the help of a script, a user can obtain unauthorized access to shared credentials. Finally, Li and Evans (2017) suggest the strategies on how to mitigate the vulnerabilities associated with the use of password managers. It is important to know the risks and how to overcome them when using password vaults because, with the provided advantages of the software, one can improve the security practices dramatically. Regarding the bookmarklet vulnerability, the authors suggest not to use the click authentication functionality. Content Security Policy is said to be a tool to protect against XSS. The CSRF issue is recommended to be fixed by the developers of the password managers by including a function of checking the Refer and Origin headers of each and every request.

There are several ways the password vaults are storing the credentials: locally on a device, such as a standalone password manager installed onto a PC, on a portable device such as mobile phone, or in the cloud at a third-party server. One of the types of standalone password managers is browser-based vault. Bojan (2017) presented the security evaluation of browser extension password managers. The study described

various attacks that are possible to be executed on the browser-based password managers due to their specific features. There are several serious security concerns raised by Bojan (2017) regarding browser-based password managers. Seemingly secure due to the encryption and password protection, the password databases provided by Chrome are accessible by some third-party Chrome applications. They present a potential security breach risk because it is possible for them to obtain passwords without authorization. Moreover, this might be done without the user being aware of the credentials being stolen. Further, the devices in possession of the user might be stolen, and it is possible to guess the password by dictionary attack if it is not very complicated. Master password acts as a single point of failure in browser-based passwords, so Bojan (2017) suggests that the security of such password vaults should be improved.

Numerous attacks can be performed by exploiting the automatic auto-fill. Sweep attacks allow hackers to obtain the credentials of the users by using iframes that were displayed in the browser pages. The password vaults do not recognize that the iframe is malicious, and thus the attackers can capture the auto-filled credentials that are inserted there instead of the legitimate site's sign-in window. Besides the iFrame sweep attack, a Window sweep attack exists. In this case, the password manager will insert the password into the pop-up window that appears on a webpage, and the attacker later collects and uses those credentials. Another variety of sweep attack is the redirect sweep attack. The attacker hijacks the webpage so that the attempt to log into a service leads to a redirection to a third-party page. Hackers have the skills to obtain the credentials by making the third-party page look legitimate, so the credential theft would happen without the user realizing that the password manager automatically fills in the login form of a malicious website. Even if the user reacts on time and leaves the dangerous page, the password is already stolen by the attacker (Bojan, 2017). Auto-fill feature was studied in relation to mobile password vaults as well. Li and Evans (2017) describe a method of implementing auto-fill functionality in portable password managers. It is a script that creates a bookmarklet, and when run, it gives the user an opportunity to insert the password into the login window. Manual auto-fill functionality is vulnerable to clickjacking, an attack that is carried out by the hacker with the help of including

various layers onto the page that the user might click instead of the original page. The example page has a legitimately looking form that had a hidden iframe that captured the passwords with the help of an overlying form. The mitigation of the vulnerability is frame busting, x-frame-options header, and content-security policies, provided by the web browsers. The mitigation strategy for such types of attack is disabling auto-fill feature due to the possibility of it to be exploited.

2.4.2 Other Security Vulnerabilities

The study conducted by Bojan (2017) focuses on the security of the KEY browser extension developed by F-Secure company. The testing showcased that the browser extension has multiple vulnerabilities that need to be paid attention to. Those vulnerabilities include improper domain matching, authorization code hack, Man in the Middle attack, unvalidated redirects, credential theft (Bojan, 2017). Password managers are able to detect the web page for which there is an entry in the password database. It is necessary to control this feature because it can be exploited. The URL of the domain is not strictly checked against; hence an attacker can disguise a malicious website, so its URL resembles a legitimate one. If the user does not notice the difference in the URLs, then the attacker has a chance to obtain the credentials if the user by accident chooses to fill in the form as prompted by the password manager.

Mobile vaults several security flaws. Boukayoua (2014) states that the security in the Android-based password vaults is compromised due to the fact that the clipboard is not hidden from any application installed on the device. The study proposes the way of copying the password from the vault into the application as a complete set of characters bypassing the Android clipboard. This is done to improve the security aspect of the password manager. Graphical passwords have security limitations as well. The graphical password manager ImageTiles is vulnerable to the capture attack. A potential hacker can record the clicks the user does when logging in. The password manager itself does not identify which tiles were clicked on logon, however, with the help of camera the sequence of tiles can be obtained. Since the password does not change after every login, it is possible to verify the sequence of the tiles, and thus hack the user's account. However, the graphical passwords are highly resistant to a phishing attack. (Stobert and Biddle, 2014). Cloud-based password vaults have also been studied in terms of security.

The security of such password managers relies on the third-party. The cloud is accessible from multiple locations over the Internet, hence there is a risk of data loss initiated from different parts of the world. There was an attack on LastPass carried out in 2015 (Vinton, 2015) that resulted in significant data loss (as cited in Li and Evans, 2017), As reported by the LastPass representatives the hackers obtained access to the password database of the company, and the credentials and other sensitive data of the customers was compromised. The attackers managed to steal the passwords, the e-mails, the salts and the reminders used for password recovery. During the leakage of the data from LastPass password storage, the cryptographic hashes were stolen as well, and this could lead to the attackers being able to attempt the decryption of the credentials. The common mitigation strategy implemented by the password vault companies against such types of attacks is not to keep the master password but to use a slow key derivation function. Such a method makes it complicated for an attacker to perform a brute force or a dictionary attack on the encrypted credentials.

Table 2 presents a summary of common attacks on password managers.

Table 2. Attacks on password managers

Affected feature	Attack type	Mitigation	Source
Autofill	iFrame sweep attack, window sweep attack, redirect sweep attack, clickjacking	Disabling autofill feature, frame busting, x-frame-options header, content security policies	Bojan, 2017 Li and Evans, 2017
Domain detection	Improper domain matching	Making sure the URL of the domain is legitimate before inserting the credentials prompted by the password manager	Bojan, 2017
Android clipboard	Credential theft by a third-party application	Bypassing the android clipboard	Boukayoua, 2014
Master secret	Master key theft	Creating a complex master secret using multi-factor authentication for vault	Li and Evans, 2017
Authorization	Excessive rights for unauthorized users	Proper configuration of the software and vulnerability fixes from development	Li and Evans, 2017
Bookmarklet	Malicious page masqueraded as legitimate	Avoiding click authentication	Li and Evans, 2017
Use of vaults for authentication in WWW	XSS attack, CSRF vulnerability	Content security policy, checking Refer and Origin headers of the requests, needs to be implemented by developers	Li and Evans, 2017
Chrome browser password manager	Attack through a third-party Chrome application	Avoiding third-party application in Chrome	Bojan, 2017
Graphical password management	Capture attack	Ensuring there is nobody overlooking the clicks and is not recording the movement of the mouse	Stobert and Biddle, 2014
Third-party storage	Credential theft	Slow key derivation function to protect the client credentials against decryption, biometric authentication, two-factor authentication	Yang et al, 2014

The research conducted by Yang et al (2014) suggests that besides using the master password to protect the vault, alternative solutions with a more enhanced security are

available. Biometrics and two-factor authentication provide the users with a multi-layered security solution to protect the credentials stored in password managers. However, the study focuses primarily on the cloud-based password vaults, where some of the tokens and biometric features are not compatible. Moreover, biometric authentication raises concerns about privacy. Some people do not want to provide the biometric identifiers to a third party.

2.4.3 Vulnerability Mitigation Strategies

Various solutions were presented by different studies in order to enhance the security of password managers without compromising usability. The study by Yang et al (2014) is aiming at investigating whether it is possible to combine the security, ease of use and privacy options in order to deliver a cloud-based password manager solution that would satisfy the needs of the users. In order to achieve that, a scheme has been suggested with the implementation of Single Sign-On and Biometric Template Protection, or BTP. The technic of biometric data protection is aimed at the privacy of such data, for example, retina or fingerprints. BTP changes the biometrics so that it is saved in a form of a secured template by using a particular function with the help of a key that is assigned to the user. The suggestion of Yang et al (2014) is to implement biometric authentication method as a part of the two-factor authentication. First, the user will need to input a master secret, and as a second step, the biometrics will be matched against the ones stored in the database. The process is intended to be done as a whole, to eliminate the opportunity for the attacker to learn which of the steps led to a failure in authentication. Moreover, the manner storing of both the biometric information and the master key is ensuring that in case one of the authentication keys is stolen, the other will preserve secured. Finally, the study claims that the password manager using such type of two-factor authentication can be done in combination with the scalability and accessibility of the cloud-based password managers. The authors (Yang et al, 2014) are hoping that the suggested model can enhance the security of cloud-based password vaults without compromising the usability of them.

In an attempt to develop a secure online password manager, Englert and Shah (2009) conducted a research in which they presented a software that gives an opportunity for the user to save their credentials in an online database securely. The vault is claimed to

be convenient due to its accessibility from across the network. Moreover, the credentials are transmitted over the internet in an encrypted way in order for the attackers not to be able to capture the traffic and obtain the passwords of the users. The Greeting mechanism is being introduced as a method to prevent phishing attacks on the system. A list of 'known' or 'trusted' hosts are provided by the user to the server, and thus the access is limited by the configured IP addresses. When the user accesses the server from an authorized location, a greeting message is shown, and if it is recognized by the user, then the next step is to go to the page. The design by Englert and Shah (2009) suggests that the user would have to provide three variables: username, password, and a secret key. Moreover, it will be necessary to report whether the source computer is intended for personal or public use, in order to be able to decide whether to add the IP of it to the trusted hosts on the server.

The design suggested by Englert and Shah (2009) is expected to protect the user against phishing. This type of attack is aiming at obtaining user's credentials through a page that looks exactly like the original one (Englert and Shah, 2009). The attacker is designing a page so that the user thinks that it is an original one, and therefore enters the credentials. The domain name might resemble the legitimate one, and the design of the page makes the user think that it is safe to input the credentials. However, if there is a custom greeting message presented to the user, it is possible to realize when the website is legitimate or not, thus eliminating the risk of providing the credentials to fake webpages. It depends solely on how attentive the user is because an attacker might attempt to present a default or a similar kind of a greeting message or eliminate it completely. Setting the trusted hosts eliminates the chances of the adversary to be able to see the customized greeting message, therefore it will be almost impossible to create a message similar to the original one in order to trick the user into providing the credentials. Such a solution of a password manager is designed to mitigate multiple attacks by providing a complex design that allows the user to set up limited access to the database.

2.5 Usability Issues of Password Managers

A common desire of users is to have convenience in their everyday life (Schougaard et al 2016). Various studies have been conducted on the usability of different password

managers. Moreover, multiple prototypes have been proposed in an attempt to improve the usability of password managers without compromising the security of the software. Table 3 presents the common usability concerns regarding password managers.

Table 3. Usability concerns of password managers

Functionality	Usability concern	Suggested improvement	Source
Accessibility	Possibility to access the password manager from various locations	The use of cloud-based password managers	Schougaard et al, 2016
Authorization	Allowing multiple users to access the database without compromising security	Authorization hierarchy	Li and Evans, 2017
Organization	Being able to easily locate the needed credentials	Structuring and organizing the credentials	Schougaard et al, 2016
Device compatibility	Installing the same software on different devices and operating systems	Cross-platform password manager	Schougaard et al, 2016
Control over credentials in the cloud	The opportunity of fully administering own credentials	Private cloud with full administrator rights	Schougaard et al, 2016
Development of password vault	The opportunity of developing the password manager according to the needs	Providing the user with opensource and licenses needed for developing the software	Schougaard et al, 2016
Help with password requirement compliance	User needs to have real-time control over the password creation to meet the requirements	Showing the amount of characters while the user is entering them	Tannen et al, 2019
Case-sensitivity	Case-sensitivity leads to many mistakes and worsens the user experience	Removing case sensitivity	Tannen et al, 2019

There are certain requirements for the security software to be considered usable: acknowledging the requirements that need to be completed in order to ensure the security of the performed tasks, having an understanding how to achieve the successful completion of the tasks without completing any errors, feeling comfortable when operating the software Chiasson and Oorschot (2006). In addition, the study (Chiasson and Oorschot, 2006) suggests that it is equally important to make sure the users understand whether the task has been accomplished and getting the information about the system status. The main goal of the authors is to raise awareness of how lack of usability might compromise password security in very serious ways. The problems

regarding usability in password managers not only prevent the users from adopting them but also when the technology is used incorrectly, it can harm the security even more. The study suggests that there should be a more thorough study done that would help understand how the usability problems can be solved, and possibly have a developed prototype of a password vault that has the usability shortcomings addressed and fixed. Table 3 summarizes the findings related to the usability of password managers.

2.5.1 Usability and Accessibility

The advancement of technology and society led to the need of the password database to be accessible from multiple devices and locations, which further led to the use of cloud-based vault. The study conducted by Schougaard et al (2016) focuses on the cloud-based password vaults, as they suggest better accessibility of the password database. However, there are a few shortcomings of such a solution. The aforementioned research describes the main functional requirements of the cloud-based password vaults, which include accessibility as the main function. Moreover, it is necessary to have a hierarchical authorization structure, so that different users have different access rights to the database. Furthermore, there is a need for a convenient organizational structure, so it is easy to find the necessary credentials and achieve good user experience. The database should be cross-platform, so the user is able to access the database from any type of device and using different software. There is a need to have the functionality of doing various operations with passwords, and it is absolutely essential for the credentials to be encrypted, so it is not possible for an attacker to obtain the sensitive information of the user (Schougaard et al, 2016). The study also suggests that there are several non-functional requirements that need to be considered in a cloud-based password manager. It is important for the user to store the passwords in the systems where they can have full administration rights. Such a system as a private cloud is an appropriate solution in this case. The authors (Schougaard et al, 2016) also argue that the user would benefit from a possibility to develop the password management system. Hence, the opensource and licensed software could be a valuable asset for the cloud-based password vault. There may be a further need for the user to increase the amount of entries in the database by a significant amount, therefore among other non-functional requirements, Schougaard et al (2016) mention the scalability. The authors also mention the

standardization such as setting encryption and latency requirements for the improvement of password vault security and user experience.

The aforementioned study by Schougaard et al (2016) covered 14 major cloud-based password managers. The analysis showcased how those password vaults fulfill the functional and non-functional requirements. The shortcomings of the studied software were that most of the products were oriented towards corporate use rather than individual adoption. The suggestion was made by the authors of the study to allow the users to have a personal folder available under their own credentials where they could store and manage their personal passwords. Most of the vendors were reported to provide the users the possibility to operate the software on different platforms according to their preference. However, this was mostly possible for the password manager service rather than the actual database. Finally, Schougaard et al (2016) concluded that none of the cloud-based password vaults fulfilled the initially stated requirements that were claimed to help achieve better usability and user experience. The authors argue that there is no perfect cloud-based password manager available currently on the market, even though the portability and accessibility of such vaults have a significant positive impact on the usability and user experience.

2.5.2 Usability and Software Adoption

A brief study of Tannen et al (2019) discusses the usability of four password managers from different vendors. A group of professional usability testers analyzed the vaults against thirteen criteria. The study was aimed at investigating the aspects that influence the user experience and successful adoption of password managers. A set of tasks was required to be completed from the participants of the study with the help of password managers. The tasks included logging in, changing the password, creating security questions for password recoveries, and synchronization of the credentials among different platforms and systems. The study claims that usability testing resulted in 25 suggested usability improvements. Some of them were described more specifically, such as showing a real-time amount of characters while the user is in the process of creating the password. This feature is expected to help the users see whether the requirement regarding the password length is met. Furthermore, the testers suggested to remove the case-sensitivity from the passwords. It is expected that case-sensitivity is a

feature that increases the chances of the users to forget or mistype the credentials. However, the drawback of removing such functionality affecting the security and the complexity of passwords, since there are fewer character combinations (Tannen et al, 2019). The study suggests that it is challenging yet possible to combine the usability and security. In some cases, however, improvements aiming at ease of use might be implemented at an expense of security.

A study conducted by Chiasson and Oorschot (2006) investigates the usability of two password managers, PwdHash and Password Multiplier. A total of 26 users participated in the research, where they were prompted to perform different tasks with the password vaults and the feedback was collected afterward. Moreover, the researchers observed the non-verbal reaction of the participants. The same tasks were requested to be completed on both password managers. Prior to the testing, the researchers collected the background data from the participants related to their security practices online, and how they operate their passwords. The study suggested four different tasks to be performed during the testing phase: setting up entries in the password manager for the future use, logging into a system with the help of the password vault, complete the procedure of changing the password for some account, and access the accounts from a different location than the primary device. While the users completed the required operations, a dedicated examiner was observing how they react to the tasks. There were five main categories of the result of each operation: 1) successful completion of the task, 2) dangerous success that meant that the user struggled to complete the task,3) failure, 4) false completion that meant that the user thought the task was completed successfully, whereas, in reality, the task failed to be completed, 5)and the last category is failure due to an incorrect completion of a previous task.

The study indicated that there was quite a low success rate for performing the requested tasks. Four out of five tasks were completed with the success rate below 50%, which raises a serious concern regarding the usability of the studied password managers. The examiners were carefully following the emotions and reactions of the participants, which is expected to help understand the causes of failures better. The research claims that users had difficulties with activation of the software, and they also misunderstood

how the security functionality was implemented in the password manager. The participants were often mistakenly considering that their actions were benefitting to the security, although they have failed to change their weak credentials to more secured ones. The false perception of security could harm the users and result in a serious data loss. Moreover, the participants falsely assumed that the passwords were regenerated every time they enabled the password managers. The usability issues discovered throughout the research were caused both by the password vaults and by the poor design of the websites that were involved in the study. Thus, the researchers argue that there are environmental factors that can seriously impact the user experience in a negative way when an individual decides to use the password manager. There was also inconsistency observed regarding the naming convention for usernames, thus the participants of the study had doubts when using the interface of a password vault and the websites. Multiple cases of users being frustrated with the software complexity were reported and observed. The participants did not feel that they had control over their passwords since they were not available for the users to be created or seen. This functionality is assumed to be preventing the participants from sharing the credentials in a less secure way, for example writing them down on a piece of paper. Lack of trust was mentioned in the research as well: people claimed that they had difficulties relying on software when dealing with such a sensitive topic as personal credentials and protecting sensitive data. The feelings reported by the participants of the study and security recommendations are opposite to each other. The users reported that they have no doubts managing their passwords securely in an alternative way than using a specially developed software.

2.5.3 Usability and Security

The research described by Chiasson and Oorschot (2006) points out an important fact: sometimes lack of usability can lead to serious problems with security. If the users do not understand how the password vault works, they might accidentally expose themselves to an attack. The participants of the study repeatedly forgot how to activate the password vaults. Some users failed to change the passwords, so they ended up reusing their old credentials. Moreover, some participants were not able to activate the software, and they were trying to recall their credentials. With the help of a phishing attack, a hacker would get an opportunity to obtain several variations of passwords the

participants had in mind, hence expanding the database of possible credentials that could help get access to some account of the user. Finally, the participants were observed to be in favor of easy-to-guess passwords due to the fact that they relied on the complete security of a password manager as a mechanism that would protect their credentials from being stolen.

There are password managers created specifically for mobile devices, and usability of such kind of vaults is more challenging due to a smaller size of the screen (Boukayoua et al, 2014). Moreover, the user has to switch between applications when using the password manager, in order to input the password from one application to another. Chiasson and Oorschot (2006) suggest various improvements for the usability of password managers in order to improve the user experience and assure the secure usage of the technology. First and foremost, the users must understand when their credentials are being secured. The individual should also understand whether the software is on or he needs to perform some actions in order to trigger it; the actions have to be easily understood by the user as well. It must be clear for the people who decide to take up using password vaults, how to change and move the credentials from and to password manager, and if the user commits a mistake when using the software, there should be short and clear cues how to avoid or correct the error. Finally, it is important to provide the users with more transparency regarding whether the credentials for certain accounts are being secured. The authors claim that the satisfaction and acceptance are the key factors that are affected by usability.

2.6 User studies on Password Managers

There have been previously conducted studies in relation to the adoption of password managers among different target groups of people. The study by Fagan et al (2017) focuses on the principal reasons for the users to adopt or not to adopt the password managers for the regular use. The purpose of the study was to address the concerns of the non-users towards the adoption of the tool by identifying the main reasons why they choose not to use the software for managing their passwords. The findings lead to an assumption that many users do not have a full understanding of the password managers' functionality. Those who do not use password managers claim that the tool lacks security, due to the fact that all the passwords are obtainable in case the hacker gets the

password manager unlocked. The research identified that the users of the password managers claimed to use more accounts and use them more frequently. Moreover, the respondents that have more passwords, reported that they find password managers useful.

There was an open question asked in the study by Fagan et al (2017) in order to identify why users decide not to choose password managers to manage their passwords. For users, the main reasons in favor of using password managers are convenience – 80% respondents, security – nearly 25%, and 1% of responses were classified as 'Other'. The non-users reported lack of need – nearly 42% of the responses, lack of time and motivation – nearly 11%, and inconvenience and lack of usability – 9% of responses. The study does not cover the difference between the people who had never heard of password managers, and those people who knew about the software but decided not to use it. It is an important shortcoming because the people who do not know about password managers might decide to use it later once they get familiarized with technology.

Another study conducted regarding the password managers was done by Arias-Cabarcos et al (2016). The research is based on the four most popular password managers: LastPass, KeePass, Dashlane, 1Password. They were analyzed from the perspective of usability and security. The study concludes that the security and the usability tests were rather positive, which points out the potentially successful adoption of the password managers in the foreseen future. The further studies suggested by the paper are the ways to implement the password managers' use in companies by enforcing it through the security policies, combining SSO and password managers, and eventually improving the usability of the password managers. Another major suggestion in the paper is developing a software that could evaluate the security of the password managers in order to assess the possible vulnerabilities and risks related to the use of the software. The further direction from the study could be investigating further on the effect of usability and security on an intention to use adopt the password managers, and the further adoption of the technology for daily use.

Aurigemma et al (2017) analyzed the adoption of password managers as well. The paper discusses the reasons why the users do not choose password managers to store their passwords and why the software is not widely adopted despite its acknowledged functionality and benefits. The following main factors that prevented the users from adopting the password managers were identified after the study (Aurigemma et al, 2017):

1. Insufficient Time: respondents claimed that they did not want to dedicate some time specifically to install and configure the password manager
2. Excessive Effort Expected: the users claimed that it takes an extra effort to use the password manager on every login
3. Lack of Immediacy: the respondents did not start using the technology even though they intended to, because they got distracted, and eventually forgot to come back to try the new technology out.
4. Low Self-efficacy: the respondents were unsure if they are skilled enough to perform the password manager installation and be able to use it
5. Threat Apathy: the users do not acknowledge the severity of risks related to poor password management
6. Alternative Solution: many respondents have chosen a different method to manage their passwords, which does not involve an application dedicated to it
7. Lack of Trust: participants did not want to rely on the security of the password managers.
8. Insufficient Awareness: the respondents have not obtained enough information previously in order to decide on whether to adopt the password managers for their everyday use or not.

The paper further divides the above factors into three main groups: individual inhibitors – insufficient time, lack of immediacy, excessive effort, and low self-efficacy; threat apathy and technology inhibitors – alternative solution, lack of trust, and insufficient awareness.

The research by Aurigemma et al (2017) is intended to raise awareness of the users regarding the security risks associated with poor password management, as well as

creating a framework to provide the users with an effective training on installation and use of the password managers in order to eliminate the factors of time insufficiency and lack of immediacy. The article also discusses the possibility to reduce security issues by adopting the password managers widely, so it is important to understand the factors that prevent users from doing so.

Maclean and Ophoff (2019) conducted a study on factors preventing the users from adopting password managers. The research was done with the help of UTAUT2 model and targeted people working in the field of IT and technology, as well as students and staff at one of the South African universities. It was discovered that performance expectancy, as well as habit and trust, are the main aspects that lead to the people's intention to adopt password managers. However, the study did not include the correlation between the factors and the actual adoption of the software, only the behavioral intentions was taken into consideration.

2.7 Theoretical Models Related to Technology Adoption

Technology adoption is quite a popular topic nowadays due to the fact that there are multiple technology-based services available for users, and developers need to understand which areas need to be paid attention to in order to make their product more attractive for the end-user. Technology adoption refers to the process of using a certain technology for carrying out particular tasks (Ferratt and Vlahos, 1998). It is necessary to take into consideration many factors that affect the use of technology. According to Chinchor et al. (2012), the evaluation of the technology effectiveness should be based on a combination of different factors besides, the study suggests that the factors that lead to the technology adoption go beyond usability. An important question regarding technology adoption in the context of security is whether the behavioral intentions lead to the adoption of security practices. Egelman et al (2016) studied the relationship between the desire of the users to follow certain security practices and the actual degree to which the individuals adopted the security behavior. The outcome is limited in scope but points to the conclusion that it is highly likely that the behavioral intentions actually lead to the user adopting security practices. The thesis research will be focusing on behavioral intentions and adoption of the password managers, in order to find out what aspects influence the behavioral intentions, and furthermore, whether the intentions

have an actual effect on the further adoption of the software by the students in Europe. There is a need for a complex approach to the problem, in order to identify the reasons why an individual would decide to use or not to use a certain technology for daily operations. There have been multiple theoretical models developed in relation to the technology adoption. However, as discovered during the literature review, there was no study previously done on password manager adoption by using any of the theoretical models tailored for technology adoption.

2.7.1 United Theory of Acceptance and Use of Technology

United Theory of Acceptance and Use of Technology was defined by Venkatesh et al (2003). The UTAUT model derived from the Technology Acceptance Model, or TAM (Davis, 1989), and is now the most well-known and popular variation of TAM. The UTAUT model combines TAM, Theory of Planned Behaviour and Innovation Diffusion Theory, social cognitive theory and motivation model (Negahban and Chung, 2014). The model consists of four major constructs, such as performance expectancy, effort expectancy, social influence and facilitating conditions (see Figure 1). These variables are independent of each other.

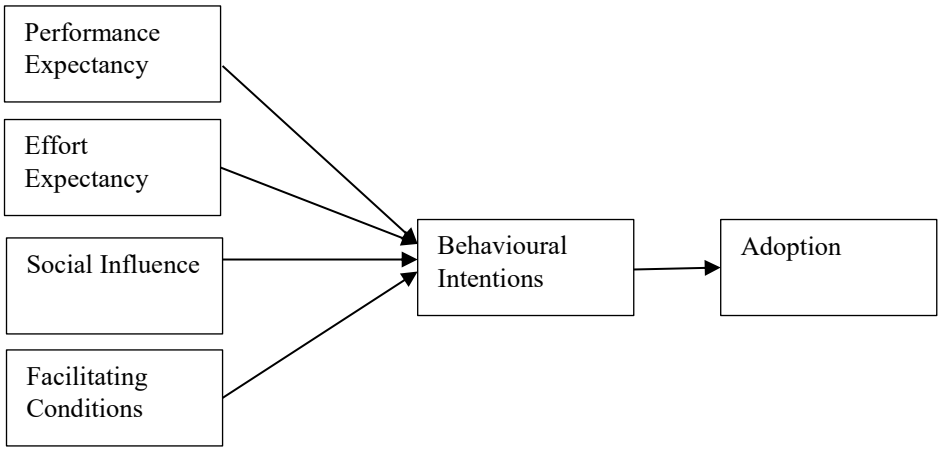

Figure 1. UTAUT model

The model also takes into consideration the motivation of the individual, both internal and external (Negahban and Chung, 2014).

Different researchers have defined UTAUT constructs differently. Synthesis of such definitions are given in Table 4.

Table 4. UTAUT constructs

Construct	Definition	Source
Performance Expectancy	"Degree to which an individual believes that using the system will help him or her to attain in job performance"	Venkatesh et al, 2013
	"The extent to which individuals are convinced by the fact that utilizing the system will help them to achieve benefits in the execution of their job"	Magsamen-Conrad et al, 2015
	"The belief that using a particular innovation will lead to positive outcomes"	Casey and Wilson-Evered, 2012
Effect Expectancy	"Degree of ease associated with the use of the system"	Venkatesh et al, 2013
	"A user's subjective evaluations of ease of engaging with an IT system"	Magsamen-Conrad et al, 2015
	"A user's subjective evaluations of ease of engaging with an IT system"	Casey and Wilson-Evered, 2012
Social Influence	"Degree to which an individual perceives that important others believe he or she should use the new system"	Venkatesh et al, 2013
	"The extent to which individuals's perceptions that the people who are close to them or those who hold important positions in their life believe that they should try using the new system"	Magsamen-Conrad et al, 2015
	"Degree to which an individual perceives that it is important for others to believe that he or she uses the new technology or complies with other's expectations'	Oliveira et al, 2014
Facilitating Conditions	"Degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system"	Venkatesh et al, 2013
	"The extent to which individuals consider that there are certain technical and organizational conditions existing that help facilitate the use of the system"	Magsamen-Conrad et al, 2015
	"The level of accessibility to technological and organizational resources that facilitate the use of the IT system"	Casey and Wilson-Evered, 2012

Performance Expectancy

Performance expectancy is explained as the extent to which the user considers the technology to be a valuable asset to the performance in daily tasks. According to Venkatesh et al (2003), performance expectancy is the major construct that can help foresee further technology adoption. The construct was originally defined as perceived usefulness in the TAM model. Furthermore, Motivation Model describes the predecessor of performance expectancy construct as extrinsic motivation; Innovation

Diffusion Theory defines performance expectancy root construct as relative advantage, and finally, Social Cognitive Theory includes one of the predecessors of performance expectancy in construct outcome expectation (Magsamen-Conrad et al, 2015). Multiple studies done using the UTAUT model show a significant relationship between performance expectancy and behavioral intentions to adopt various technologies (Oliveira et al, 2014, Magsamen-Conrad et al, 2015, Casey and Wilson-Evered, 2012).

Effort Expectancy

Effort expectancy is a metric that is describing how easy it is for the user to operate the software. Research by Taiwo and Downe (2013) claims that show that the construct does not show much significance in explaining behavioral intentions (as cited in Magsamen-Conrad et al, 2015). However, a study by Diño and de Guzman (2015) showed that when dealing with the older group of adults effort expectancy was important for investigating the intentions of adopting a certain technology (as cited in Magsamen-Conrad et al, 2015). Effort expectancy is described as a significant construct of UTAUT in case of compulsory and voluntary technology usage. However, it is noted that during the initial usage of the technology the factor is more important, but after some time it loses its significance in explaining technology practice. Moreover, it was suggested that effort expectancy factor is more significant among women rather than men, and for older working individuals (Venkatesh et al, 2003).

Social Influence

Social Influence is the construct defined by the importance of social opinion whether the individual should use the technology. There are several root constructs that were the predecessors of social influence: subjective norm, social factors, and image. Magsamen-Conrad et al (2015) claim that the construct does not show significance in explaining behavioral intentions. The variable includes the perception of the public image improvement when the technology is adopted, as well as the opinions of the closest people on whether the individual should be using the software. Social influence also includes the perception of being penalized in case the behavior does not meet the desired norms. However, prior literature highlights that social influence is important in the context of compulsory usage of technology at the early stages.

Facilitating Conditions

Facilitating conditions factor is described as "degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system" (Ventakesh et al, 2003). Facilitating conditions construct derives from perceived behavioral control, compatibility, and facilitating conditions of Model of Personal Computer Utilization. The variable is a combination of the perceptions regarding the available facilities and technological resources that could help in using the software. Furthermore, assistance from a professional and provided support are considered as a part of facilitating conditions. Moreover, the technology should match the experience, necessities, and ethics of the individual.

Application of UTAUT in Research

The model, as stated by Ventakesh et al (2003), is not sufficient as the source of information for the software designer when analyzing the individual acceptance of technology. The article suggests that the UTAUT model should be used in combination with various different models to achieve a more accurate result. Moreover, it would be beneficial to have the model tested against different demographic groups, on different technologies, and in different contexts.

UTAUT model has been used in multiple studies regarding the adoption of new technology. Ting and Deng (2012) used the UTAUT model to determine the main factors that influence the decision of the individuals on whether to adopt the use of mobile e-books. The study suggested to include an additional variable – perceived cost. This was done due to the fact that mobile books are paid by the user, and this might affect the adoption due to the financial condition of the individual. Moreover, it was suggested that there should be a path added within UTAUT, that describes the influence of effort expectancy on performance expectancy (see Figure 2). The study also suggested to include a path from Social Influence construct to Performance Expectancy. It was believed that these two variables have a dependency on each other.

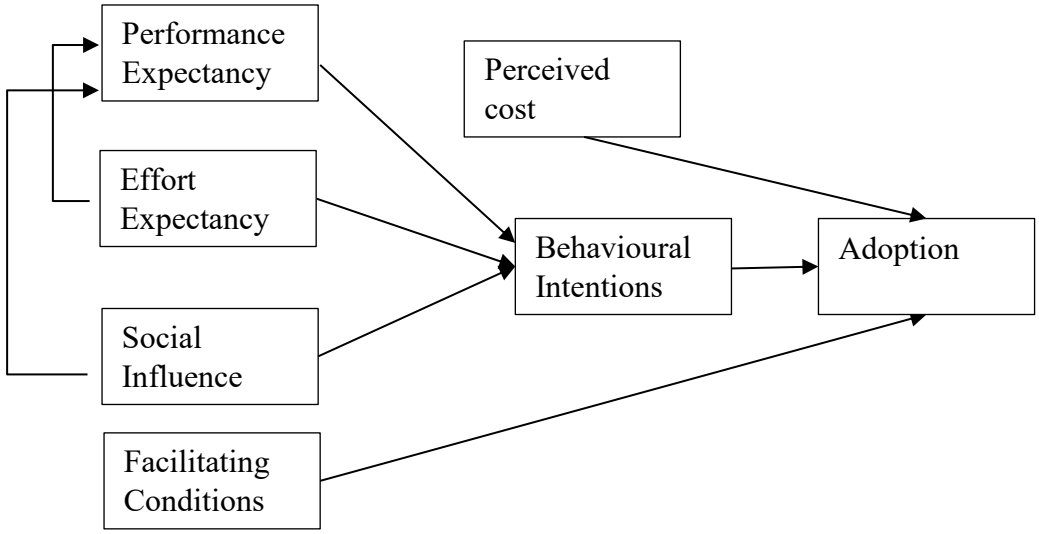

Figure 2. Modified UTAUT Model. Source: Ting and Deng (2012)

The outcome of the research showed that performance expectancy has quite an important impact on the behavioral intention. Furthermore, effort expectancy has both direct and indirect impact on behavioral intentions. Finally, the facilitating conditions and perceived costs showed no influence on the adoption of the mobile e-books. However, social influence was proven to have a positive impact on performance expectancy. Therefore, the adjustments made to the UTAUT in the study were proven to be important for a wider picture of adoption of mobile e-books.

Another study with the use of an enhanced UTAUT model was done for analyzing the adoption of mHealth adoption among the elderly population of Bangladesh (Hoque and Sorwar, 2017).

Figure 3 demonstrates the updated model.

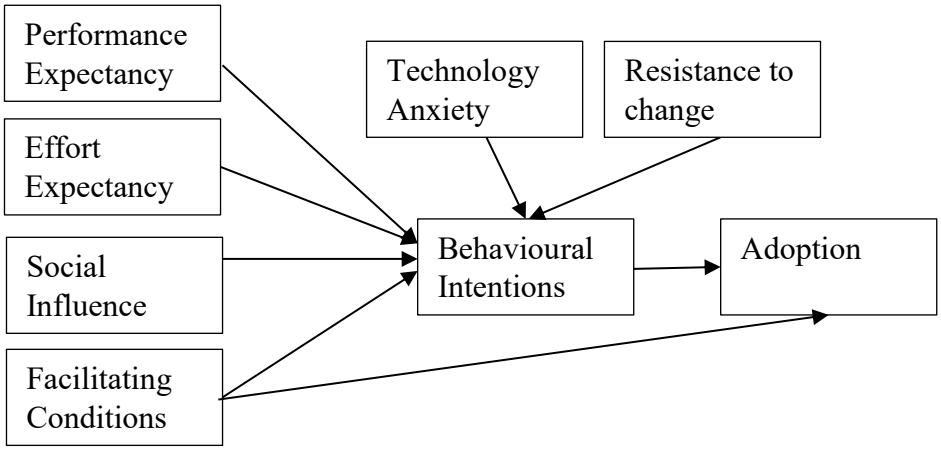

Figure 3. Modified UTAUT Model. Source: Hoque and Sorwar (2017)

There are additional constructs added: technology anxiety and resistance to change. Moreover, a new path was suggested to analyze the impact of facilitating conditions on the behavioral intention in addition to the user behavior. The results of the empirical test showed that performance expectancy, effort expectancy, and social influence have a positive effect on behavioural intentions. Moreover, the hypotheses related to technology anxiety and resistance to change were confirmed, these two factors negatively impact the behavioral intentions to adopt mHealth. The study was limited to a certain population category; hence it would not be possible to understand the factors affecting the adoption of mHealth globally. The constructs technology anxiety and resistance to change are characteristic to an elderly population. However, the study proves that it is possible to use the model for studies related to mHealth technology adoption.

2.7.2 Task Technology Fit Model

Task Technology Fit (TTF) is a model derived from the Technology Acceptance Model (Davis, 1989). TAM facilitated the research related to the use of technology. It helps to predict the adoption behavior related to technology. The model is based on two constructs: perceived usefulness and perceived ease of use (Daradkeh, 2019). Perceived Usefulness is described as a subjective perception of the user towards the usefulness of the technology for everyday tasks. Perceived Ease of Use is defined as the expectation

of the user regarding the effort necessary to operate the technology (Daradkeh, 2019). TTF is expanding the TAM model. TTF or Tack Technology fit adoption model proposes that in case the technology allows to complete the daily operations in an efficient manner, a user will consider adoption of such technology. This suggests that the adoption of a particular technology depends greatly on the tasks the user carries out on a daily basis (Goodhue and Thompson, 1995).

There are three categories of tasks defined by Gebauer et al (2010): operational, leadership, and informational and knowledge tasks. The model uses four components in order to illustrate the acceptance of the new technology: task characteristics, task technology fit, technology characteristic, and use. Figure 4 presents the TTF model and the relationships between constructs.

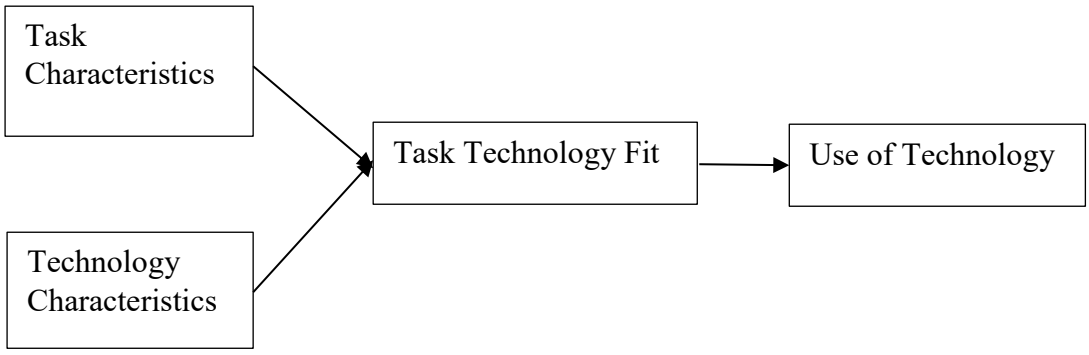

Figure 4. Task Technology Fit model. Source: Goodhue and Thompson, 1995

The characteristics of the technology and the tasks help determine the task technology fit, which leads to the decision whether to use or not to use the technology to execute daily operations. Another definition, suggested by Daradkeh et al (2019) is describing tasks as activities, that people engage in on a daily basis for business purposes, such as decision-making and analysis, for which they use technology as a tool. TTF is showcasing the relationship between the task requirements, user capabilities and the functionality of the technology, and how the aforementioned qualities influence the adoption of the certain technology for performing the tasks. The model presented by Goodhue and Thompson (1995) is suited for the individuals. Zigurs and Buckland (1998) adapted the model to fit the groups. Daradkeh et al (2019) mention that there are

multiple variations of the TTF model used nowadays. The study done by Daradkeh et al (2019) was done on the adoption of visual analytics tool using a combination of TAM and TTF. The findings of the study showed that the higher the ease of use and the usefulness were, the higher the value of TTF was reported. Task Technology Fit model was also used to study the adoption of cloud-based collaborative learning technologies (Yadegaridehkordi et al, 2014). Figure 5 demonstrates the model used in the research by Yadegaridehkordi et al (2014). The study was conducted among the undergraduate students in Universiti Teknologi Malaysia which is a similar target group as in the current study.

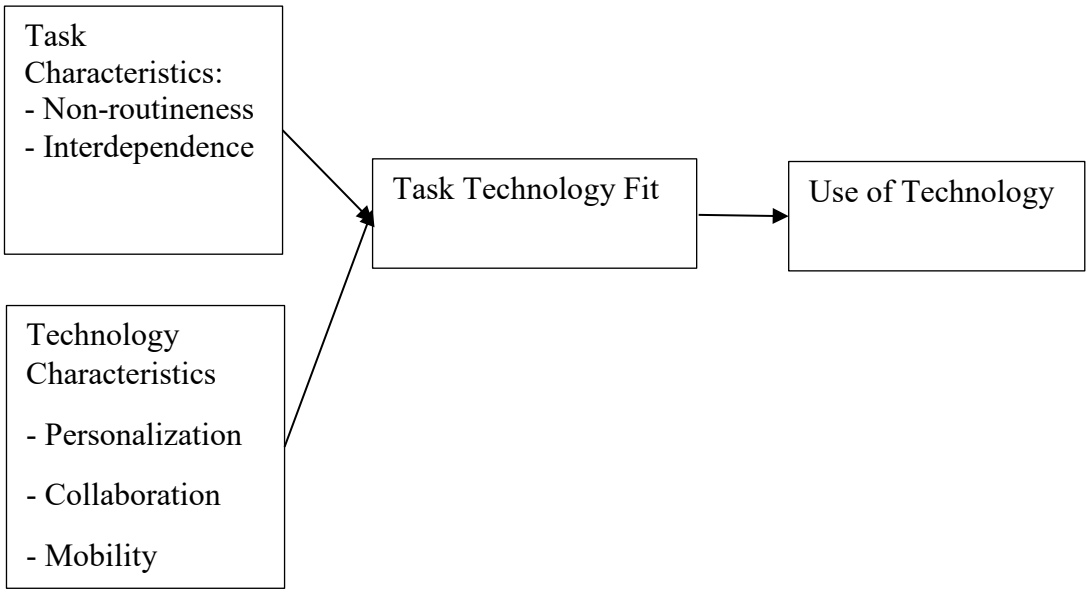

Figure 5. Task Technology Fit model (Yadegaridehkordi et al, 2014)

Task Characteristics were divided into the following sub-variables: task non-routineness and task interdependence. Technology Characteristics consist of personalization, collaboration, and mobility constructs. The analysis was done with the help of the SmartPLS tool. The results proved that task interdependence showed no statistical significance in explaining task-technology fit. However, the remaining sub-constructs were proven to be positively influencing task technology fit, and subsequent adoption of cloud-based collaborative learning technologies among undergraduate students of the Malaysian University of Technology.

3 Methodology

3.1 Integration of UTAUT and TTF

Several successful attempts have been made to combine TTF and UTAUT models to study technology adoption from a wider perspective. Zobayer (2017) used the TTF-UTAUT model to analyze the adoption of mobile banking among people in Bangladesh. With the help of the integrated model, it was possible to analyze the relationship between the constructs of two models. Task-Technology Fit was expected to positively influence the performance expectancy regarding mobile banking. However, the model did not include behavioral intentions as a separate construct, which could be a valuable asset to the model. SPSS was used for the analysis of the collected data sample. The study showed that technology characteristics have a stronger impact on task technology fit than task characteristics. Task technology fit was proven to have a positive influence on the performance expectancy, which proved the correlations between UTAUT and TTF models.

Another attempt to analyze the adoption of technology with the use of UTAUT and TTF was done by Bozorgkhou (2014). The study analyses the adoption of internet shopping among users in Iran. In this research, the data set was analyzed against two models. The results showed no significance in explaining performance expectancy with the task technology fit constrict. Effort expectation did not show significance in explaining user adoption. Nonetheless, most of the hypotheses defined in the study were confirmed. Social impacts, performance expectancy and facilitating conditions showed a positive influence on the adoption of internet shopping.

The combination of UTAUT and TTF models was used for the investigation of the password manager adoption among students of European universities. With the help of the models, it is expected to discover the factors that may lead to the intentions of students to use password managers, as well as to determine the factors that positively affect the adoption of password managers.

3.2 Research Model

Password management is necessary nowadays due to the increasing amount of accounts and passwords people are required to use, and the security requirements for those passwords in order not to lose any sensitive data. Password managers provide the users with a way to store the credentials without the need to memorize them. People have to log into systems at work, at the university and for personal purposes, such as banking, social media, and messenger. However, not all of the users decide to adopt password managers for their daily operations, moreover, some people have never heard of password managers before. The study is aiming at answering the following research questions:

1. What is a demographic profile of a European student who (does not) use a password manager?
2. What factors affect password manager adoption among the European students?

The research model used for this thesis is a combination of UTAUT and TTF. Figure 6 presents the constructs and the relationships between them that will be analyzed in the context of password manager adoption among students in Europe.

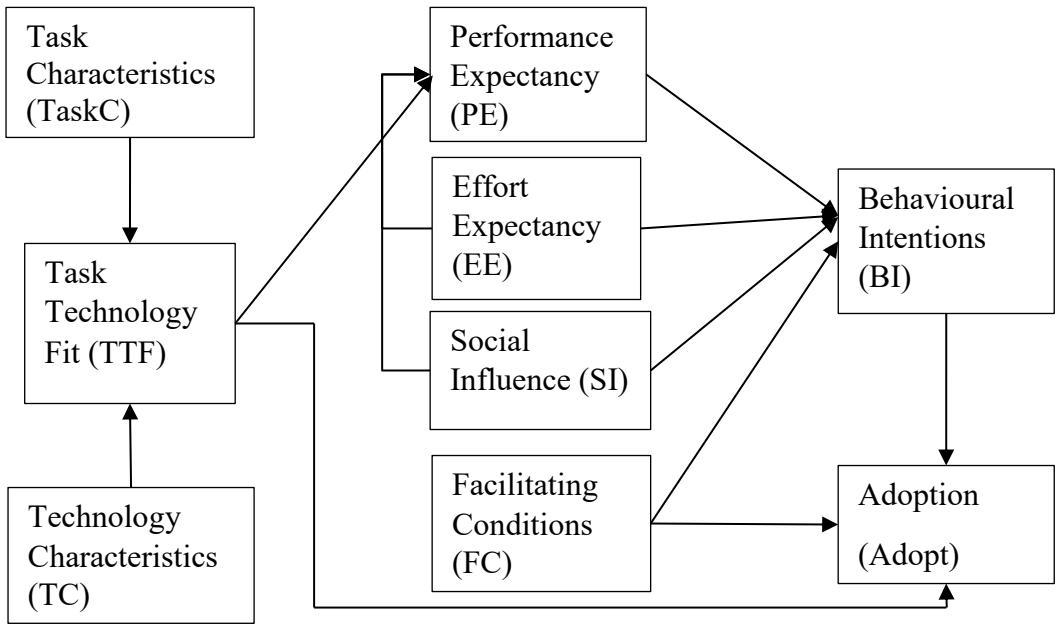

Figure 6. Study model and construct codes. UTAUT and TTF

The use of password managers has not yet been analyzed using such a framework. The study is based on multiple research papers discussing the adoption of different

technologies among different demographic categories. The TTF model tackles the task and technology characteristics and determines the task technology fit of a certain technology. UTAUT allows us to highlight the general attitudes towards the use of technology, such as effort expectancy, performance expectancy, and social influence. The same models were adapted for this thesis research: in order to identify the factors that affect the adoption of password managers. A decision was made to use the enhancement of UTAUT model done by Hoque and Sorwar (2017), and to study the relationship between facilitating conditions and behavioral intentions, as well as the adoption of password managers. However, the constructs of technology anxiety and resistance to change are specific to the elderly population, and since the study is targeting students, those two constructs were eliminated from the model. Moreover, the influence of effort expectancy and social influence on the performance expectancy were studied. This modification of UTAUT was suggested by the study of Ting and Deng (2012) in the context of mobile e-books adoption. This construct, however, is not actual for the studies on password managers since most of the provided vaults are free to install. The correlation between the TTF and UTAUT model have been previously studied in the context of mobile banking adoption (Oliveira et al, 2014), where it was proven that task technology fit construct is significant in explaining performance expectancy. Moreover, Bozorgkhou (2014) mentioned the effect of task technology fit on performance expectancy in the study on internet shopping among the users in Iran. Thus, the relationship was included in the research to find out whether it is significant in the context of password manager adoption.

3.3 Hypotheses

TTF was used in order to find out how the technology fits the daily tasks the users need to execute, and whether the technical characteristics are suitable for the further adoption and use. Fagan et al (2017) mention that convenience is a major factor affecting the willingness of the people to adopt password managers. As per the TTF model and the previous research on mBanking adoption by Zobayer (2017), as well as the study of Oliveira et al (2014) and Fagan et al (2017) the following hypotheses are formed:

H1. Technology characteristics have a positive effect on task technology fit in the context of password manager adoption

H2. Task characteristics have positive effects on task technology fit in the context of password manager adoption
H3. Task Technology Fit has a positive effect on performance expectancy in the context of password manager adoption
H4. Task Technology Fit has a positive impact on the adoption of password managers

UTAUT model is used to tackle the intentions of whether to use a certain technology. The model consists of four concepts that describe the user's intentions and behavior: effort expectancy, social influence, performance expectancy and facilitating conditions. The previous study of Maclean and Ophoff (2019) used the model for analyzing the password manager adoption among employed people. Performance expectancy identifies whether a user expects the improvement in performing his daily tasks by adopting certain technology. It is one of the most important factors for the user to decide whether to use the technology. The following hypothesis is being checked in relation to performance expectancy:
H5. Performance expectancy positively affects the behavioral intention to adopt password managers
Based on the previous research by Maclean and Ophoff (2019) as well as the study by Hoque and Sorwar (2017), and Ting and Deng (2012), the following hypotheses are checked against the target group of the thesis:
H6. Effort expectancy positively influences the behavioral intentions of an individual to adopt password managers
H7. Effort expectancy positively influences the performance expectancy of an individual regarding the password managers
H8. Social influence positively affects the performance expectancy of an individual regarding password managers
H9. Social influence positively affects the intention of an individual to use password managers
H10. Facilitating conditions have a positive effect on the intention of a user to adopt the software.
H11. Facilitating conditions have a positive effect on the decision of a user to adopt the software.

Further, the four main constructs of UTAUT as per the hypotheses may result in the behavioral intentions to use password managers, which further may positively affect the adoption of the password management software. Hence, the final hypothesis based on the UTAUT model is the following:

H12. Behavioral intentions to use password managers positively affect the further adoption of the aforementioned technology.

3.4 Measures

The variables in UTAUT and TTF models cannot be measured directly, thus each of the constructs will be analyzed through several items (Hair et al, 2017). Effort Expectancy in the context of the study is defined as the ease of use of password managers (Maclean and Ophoff, 2019), and it was represented by four different items. Performance Expectancy is defined as a level of confidence of the user that the password managers will be beneficial in performing the daily tasks. The construct was presented by 5 items. Social influence defines whether the opinion of family and friends of the respondent influences the adoption of password managers. The construct was presented by 7 different items. Facilitating conditions is the perception of the respondents whether the provided infrastructure provides enough opportunities to use password managers. Three items were used to measure the construct. Task characteristics were measured by 7 different items. The construct defines whether the respondent perceives the technology as appropriate for completing the daily tasks successfully. Technology characteristics showcase the perception of the user towards the benefits of the technological functions of the password managers. Finally, behavioral intentions were presented by 5 measurement items, and the construct was determining whether the respondent would like to adopt password managers. The Likert scale was used for measuring each of the items, from 1 to 5, where 1 was defined as ‘Strongly disagree’, and 5 was defined as ‘Strongly agree’. Table 5 shows the constructs used in the study and their definitions in the context of password managers.

Table 5. Thesis model constructs and definitions

Name of Variable	Number of items	Definition	Based on
Effort Expectancy	4	The degree to which the user considers password managers to be convenient for regular use	Goodhue and Thompson, 1995; Venkatesh et al, 2013; Oliveira et al, 2014;
Performance Expectancy	5	The perception of the individual that password managers will be useful for performing regular tasks	
Facilitating Conditions	3	The perception whether there is necessary technology and organization facilities available for the adoption of password managers	
Social Influence	7	The extent to which the user feels that the close circle of people believe it is important to use password managers	
Technology Characteristics	4	The perception of whether the functionality of password managers makes it suitable for performing daily tasks related to password management	
Task Characteristics	7	The extent to which a password manager is necessary to perform daily tasks	
Task Technology Fit	4	The perception of whether a password manager is suitable and useful for performing daily tasks	
Behavioral Intentions	5	The extent to which a respondent intends to use the password manager in the future	
Adoption	4	The degree to which the respondent uses a password manager	

3.5 Data Collection Process

The data was collected by using a popular tool for surveys Webropol, the access to which was provided by the University of Turku. The link to the questionnaire was distributed via social media, such as Facebook acquaintances, Facebook SurveyCircle group and ESN groups, acquaintance by contacting personally, and mailing lists of the University of Turku, South-Eastern Finland University of Applied Sciences (XAMK), Turku University of Applied Sciences, and Åbo Akademi University. There were multiple reminders sent throughout the two-month period while the data was being

gathered. The primary source of the responses was social media and personal contacts among current students. The design of the survey was based on the UTAUT and TTF model constructs. The variables could not be measured directly, therefore multiple questions were created for each construct. It was necessary to include multiple items per each variable due to the large data sample that was intended to be collected (Hair et al, 2017). At the end of the survey, demographic questions were presented to the participants in order to understand whether there are some differences in password vault adoption depending on the age, gender, educational background and the experience with computers and the amount of accounts used daily.

A total of 1454 respondents visited the link initially; however, out of those 312 respondents completed the whole survey. Four people decided not to participate in the survey and informed about the reasons. One of the participants stated not being a student as the motive not to proceed further with the questionnaire. Two stated the lack of time as the primary reason for not completing the survey. The last one did not provide any reason for not proceeding with the questionnaire. The study was primarily conducted in Finland, however, participants from all over Europe were invited to participate in the questionnaire, since the aim of the study was to analyze the password manager adoption among students of European universities. The participation in the questionnaire was voluntary and completely anonymous. The personal information that was collected was age, gender, field of study, the current degree level the student was obtaining. No contact details or names were collected in the process. As a measurement scale, the Likert scale was used, with the grading from 1 (Strongly Disagree) to 5 (Strongly Agree).

3.6 Data Analysis

Two models were used to investigate the factors affecting password manager adoption among the respondents are Task Technology Fit and UTAUT. The study started by verifying the distribution of the data. Eight items have a high value of kurtosis, and skewness for seven items is beyond the recommended values by Hair et al (2017). This indicates the non-normal distribution (see Appendix A). However, PLS-SEM model is suitable for a set of data with non-normal distribution (Hair et al, 2017). Therefore, PLS-SEM model was used as a method to analyze the data collected with the

questionnaire. The sample size to be analyzed is 265, therefore meeting the required amount, which is calculated as 10 times the number of arrows pointing to the construct (Hair et al, 2017). Table 6 presents the results of the analysis of constructs: outer loadings, Average Variance Extracted (AVE) and Composite Reliability (CR), as well as the t-values of the items. The items in italic were removed due to low loading values (Hair et al, 2017).

Table 6. Items, loadings, Average Variance Extracted (AVE), Alpha and Composite Reliability (CR) values. Removed items marked in italic.

Construct	Item Code	Loading	*t*	AVE	CR	Alpha
Technology Characteristics	TC1	0,771	22,561	0,656	0,884	0,827
	TC2	0,832	28,938			
	TC3	0,773	34,421			
	TC4	0,860	42,033			
Task Characteristics	TaskC1	0,756	12,235	0,734	0,892	0,818
	TaskC2	0,801	15,157			
	TaskC3	0,767	16,890			
	TaskC4	*0,495*	*5,483*			
	TaskC5	*0,493*	*5,316*			
	TaskC6	*0,019*	*0,125*			
	TaskC7	*-0,146*	*1,251*			
Task Technology Fit	TTF1	0,889	64,267	0,720	0,911	0,868
	TTF2	0,915	79,344			
	TTF3	0,835	33,378			
	TTF4	0,744	20,065			
Effort Expectancy	EE1	0,846	29,442	0,718	0,911	0,869
	EE2	0,863	38,585			
	EE3	0,899	59,850			
	EE4	0,777	25,307			
Social Influence	SI1	0,821	30,068	0,724	0,940	0,924
	SI2	0,871	48,166			
	SI3	0,898	53,295			
	SI4	0,868	54,108			
	SI5	0,828	29,310			
	SI6	0,810	24,839			
	SI7	*0,360*	*5,779*			

Table 6 (Continued). Items, loadings, Average Variance Extracted (AVE), Alpha and Composite Reliability (CR) values. Removed items marked in italic

Performance Expectancy	PE1	0,845	42,472	0,721	0,928	0,903
	PE2	0,873	47,451			
	PE3	0,865	42,385			
	PE4	0,833	35,778			
	PE5	0,827	33,972			
Facilitating Conditions	FC1	0,895	37,666	0,848	0,918	0,822
	FC2	0,922	53,445			
	FC3	*0,633*	*7,596*			
Behavioral Intentions	BI1	0,920	80,690	0,878	0,967	0,954
	BI2	*0,602*	*10,770*			
	BI3	0,960	176,284			
	BI4	0,926	51,291			
	BI5	0,924	49,590			
Adoption	Adopt1	0,986	305,153	0,973	0,991	0,986
	Adopt2	0,981	209,950			
	Adopt3	0,975	134,088			
	Adopt4	*0,619*	*10,808*			

First, the reliability and the validity of the model were tested. In order to confirm the validity of the study, the items with loading below 0.4 were removed (Hair et al, 2017). which included SI7, TaskC6 and TaskC7.

There were some items with the loading between 0.4 and 0.7, but they were not negatively affecting the validity and reliability indicators, hence the decision was made not to remove them from the model (Hair et al, 2017). Further, the items with the loadings between 0.4 and 0.7 were analyzed. As Hair et al (2017) state, it is necessary to verify whether discarding the items with the loading below 0.7 affects the validity and reliability measures. In case the deletion increases the AVE, Alpha or Composite Reliability, it is necessary to remove the item, otherwise, it should be maintained in the model. After verifying the dependability of the relationship between the construct composites and Alpha, AVE and CR, it was decided to remove TaskC4, TaskC5, FC3, BI2 and Adopt4. After removing the items with low loadings, the model reliability and validity was analyzed.

Composite reliability of all the constructs was above 0.7, which confirms the internal consistency. The average variance extracted was quite high for all the constructs, above the recommended value of 0.5. Finally, the alpha value is above the recommended threshold of 0.770, which means that the study has convergent validity and validity, which leads to the conclusion that the constructs are suitable for the model test (Oliveira, 2014). Table 7 shows the correlations between constructs and AVE values.

Table 7. Fornell-Larcker criterion. Correlations and AVE values between constructs

	Adopt	**BI**	**EE**	**FC**	**PE**	**SI**	**TC**	**TTF**	**TaskC**
Adopt	**0,986**								
BI	0,602	**0,937**							
EE	0,306	0,361	**0,848**						
FC	0,361	0,329	0,523	**0,921**					
PE	0,425	0,699	0,468	0,335	**0,849**				
SI	0,367	0,455	0,328	0,218	0,356	**0,851**			
TC	0,416	0,523	0,464	0,345	0,646	0,364	**0,810**		
TTF	0,579	0,699	0,482	0,417	0,678	0,454	0,745	**0,848**	
TaskC	0,101	0,302	0,248	0,214	0,378	0,139	0,445	0,325	**0,857**

The loadings of the remaining items in each construct was higher than the cross-loadings, and the square root of AVE has a higher value than the correlations between the constructs, which confirms the discriminant validity. The reliability and validity, as well as the internal consistency of the study, was confirmed. The results of the data analysis will be presented in Chapter 4 of the thesis.

4 Results and Discussion

4.1 Demographic Distribution of the Respondents

A total of 312 responses were collected with the help of the questionnaire. The primary analysis of the questionnaire responses identified four incomplete responses since the participants quit the survey. After further screening, three responses were removed due to the fact that the respondents were from Mexico, Canada, and China, as they did not belong to the target group. Shortly after, two people reported, that they filled in the survey despite not being students. The final report for further statistical analysis consisted of 303 entries. Despite the fact that some respondents claimed not to know about password managers, further, they responded positively to the questions about their use of the software, which identifies the inconsistency in some of the responses. Therefore, those entries were eliminated. The final data set consisted of 265 valid responses. The respondents were from 22 different European countries. The analysis of the data was done based on the demographic data reported by the respondents. Out of 265 respondents, 62% were women and 37% were men. One percent of respondents preferred not to state their gender. The majority of the respondents were aged 21-25 – 48%. Some of the survey participants were pursuing a Bachelor's degree – 44 %; 48% were undergoing a Master's degree and 8% are studying Ph.D.

Table 8 summarizes the distribution of the answers based on the demographic information.

Table 8. Demographic distribution of the responses

Factors	Distribution (N=265)
Gender	
Female	62%
Male	37%
N/a	1%
Age	
18-20	11%
21-25	48%
26-30	28%
31-35	8%
Over 35	5%
Level of Education	
Bachelor's	44%
Master's	48%
PhD	8%
Educational Background	
Law	2%
Computer Engineering	12%
Economics	17%
Education	4%
Humanities	12%
Medicine	7%
Natural Sciences	9%
Social Sciences	21%
Other Engineering	4%
Other	12%
Number of passwords used	
None	3%
Less than 5	35%
Less than 10	46%
10 to 15	13%
More than 15	3%
Computer proficiency level	
Basic	18%
Intermediate	54%
Advanced	28%

4.2 Demographic Profile of a Password Manager User and Non-User

A total of 77% of the respondents claimed to either not know about password managers or choosing not to use it. The remaining 23% of the respondents reported the use of password managers. Out of the non-users, 71% were female, 28% male and 1% did not

state their gender. Among the password manager users, 31% were female, 67% were male and 2% did not state their gender. The majority of password manager users (37%) were aged 26-30, while the majority of the non-users of password managers were aged 21-25 – 53%. The analysis of the educational level shows that most of the students that were not using password managers were pursuing their Master's degree– 47%; 46% were pursuing their Bachelor's degree, and 7% were studying Ph.D. Most of the users of password managers were also doing a Master's degree – 49%, 39% of the users are doing their Bachelor's, and 12% are pursuing their Ph.D. The educational background was analyzed as well. Among the students that reported using password managers, the majority were studying Computer Engineering - 29%. Most of the respondents that were not using password managers study Social Sciences – 25%. Moreover, the survey participants were asked the number of accounts with password authentication they need to use daily. The biggest part of respondents that use password managers in percentage was among the people that have more than 15 passwords in use – 63%. Finally, the students were asked to evaluate their computer proficiency level. The majority of respondents with basic computer proficiency level stated that they did not use password managers – 94%. Among the respondents, with intermediate computer skills, 84% did not use password managers, whilst among advanced-skilled computer users, 53% were not using the password managers. To sum up, the demographic profile of a password manager user among students in Europe is the following: a male of 26-30 years old, doing a Master's degree, studying Computer Engineering and using over 15 passwords regularly. The student who does not use password managers is more likely to be a female aged 21-25 studying Master's in Social Sciences and using less than 15 passwords. The complete demographic distribution can be found in Appendix A.

4.3 Model Testing

The bootstrapping algorithm was run against the data sample in order to confirm the hypotheses with 500 resamples and significance level 5%. Table 9 summarizes the hypotheses confirmation and the statistical data: path coefficients, T statistics, p-values and R square.

Table 9. Results of the hypotheses analysis

Construct	**Hypothesis**	**Path Coefficient**	***t***	**P Values**	**R Square**
TC > TTF	H1 - confirmed	0,748	22,749	0,000	0,56
TaskC > TTF	H2 – not confirmed	-0,008	0,179	0,858	
TTF > PE	H3 -confirmed	0,575	11,916	0,000	0,49
EE > PE	H7 - confirmed	0,179	3,825	0,000	
SI > PE	H8 – not confirmed	0,037	0,824	0,410	
PE > BI	H5 – confirmed	0,607	12,886	0,000	0,55
EE > BI	H6 – not confirmed	-0,053	1,089	0,277	
SI > BI	H9 - confirmed	0,233	5,189	0,000	
FC > BI	H10 – not confirmed	0,103	1,861	0,063	
FC > Adopt	H11 - confirmed	0,128	2,582	0,010	0,42
TTF > Adopt	H4 - confirmed	0,263	4,571	0,000	
BI > Adopt	H12 - confirmed	0,375	6,914	0,000	

The R^2 value shows that the model explains 42% of the variation in the Adopt construct. The research outcome also explains 55% of the variance in the behavioral intention construct, 49% of Performance Expectancy variation and 56% of Task Technology Fit variation. Figure 7 shows the relationships between the constructs in the model and the hypotheses; the confirmed hypotheses are marked with an asterisk (*).

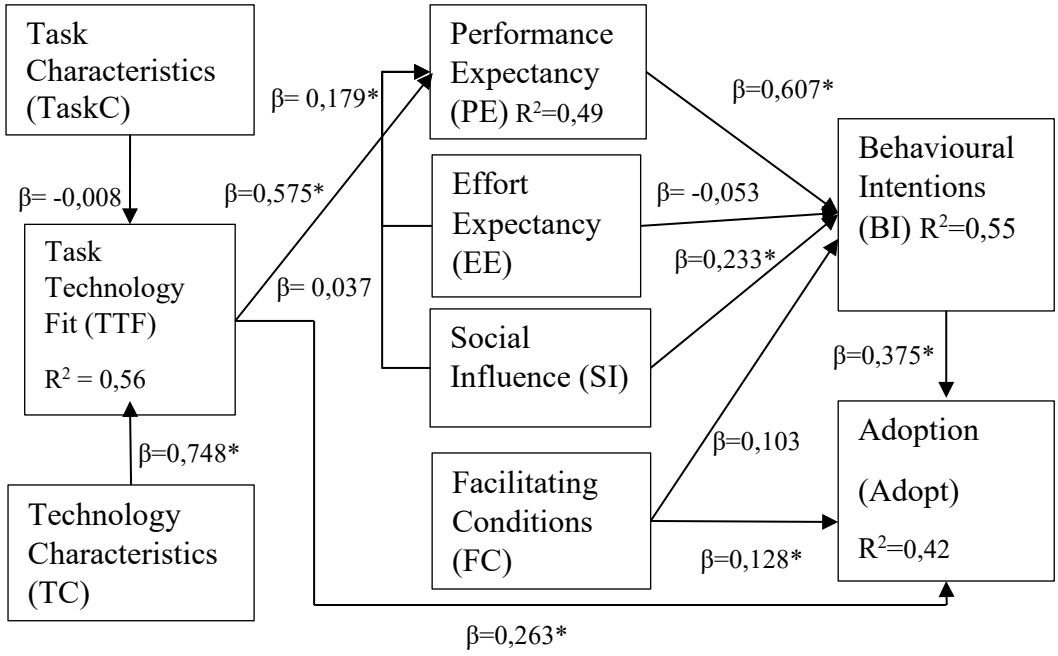

Figure 7. Construct relationship and results. Confirmed hypotheses marked with asterisk (*).

The results show that TC construct is statistically significant in explaining TTF (β=0,748, p<0,01), therefore the H1 was confirmed. TaskC construct has no statistical significance over TTF (β=-0,008, p>0,10), hence H2 was not confirmed. TTF has statistical significance over PE construct (β=0,575, p<0,01), confirming H3. TTF construct also has statistical significance in explaining adoption (β=0,263, p<0,01), which confirms H4. The analysis shows that PE has statistical significance in explaining BI (β=0,607, p<0,01), thus confirming H5. The study results show that the H6 was not confirmed since EE is not statistically significant for behavioral intentions (β= -0,053, p<0,10). Moreover, effort expectancy has statistical significance towards performance expectancy (β= 0,179, p<0,01), thus confirming H7. Social influence has no statistical significance in explaining performance expectancy (β=0,035, p>0,10), hence H8 was not confirmed by the study. Social influence construct, however, is statistically significant in explaining Behavioural Intention (β=0,233, p<0,01), thus confirming H9. H10 is not supported by the results of the analysis since facilitating conditions construct is not significant in explaining behavioral intentions (β=0,103, p>0,10). Furthermore, H11 is confirmed, as facilitating, conditions are statistically

significant in explaining adoption (β=0,128, p<0,05). Behavioral intention is significant in explaining adoption (β=0,375, p<0,01). so H12 was confirmed.

4.4 Indirect Effects

Table 10 shows the indirect effects of model constructs on Adoption construct.

Table 10. Specific indirect effects and p-values

Path	P Values
EE -> BI -> Adopt	0,294
FC -> BI -> Adopt	0,072
EE -> PE -> BI -> Adopt	0,001
SI -> PE -> BI -> Adopt	0,412
TC -> TTF -> PE -> BI -> Adopt	0,000
PE -> BI -> Adopt	0,000
TTF -> PE -> BI -> Adopt	0,000
TaskC -> TTF -> PE -> BI -> Adopt	0,865
SI -> BI -> Adopt	0,000
TC -> TTF -> Adopt	0,000
TaskC -> TTF -> Adopt	0,858

The table shows that Effort Expectancy is significant in explaining Adoption through Performance Expectancy and Behavioral Intentions (p<0,01). Social Influence is significant in explaining Adoption through Behavioral Intentions (p<0,01). Technology Characteristics are significant in explaining Adoption through the factor TTF, PE, and BI (p< 0,01). Task Technology Fit is significant in explaining Adoption with the mediating factors PE and BI (p<0,01).

4.5 Discussion

The study was aimed at finding out the factors that affect password manager adoption among students in Europe. The data sample collected with the help of the survey was further analyzed with PLS-SEM method. There were twelve hypotheses formulated for the data set, out of which eight were confirmed. The study shows that the proposed model is important in understanding the behavioral intentions in the adoption of password managers. There are certain theoretical and practical implications of the study. The analysis shows that the proposed model explains over 50% of the variation in the behavioral intention. Moreover, the study explains around 40% of variation in the adoption construct.

4.5.1 Demographic profiles of users and non-users

The research did not only analyze the responses against the theoretical models but also studied the demographic distribution of the data sample. The findings show that most of the men are aware of password managers and use them, while the majority of students that do not use password managers are women. Moreover, the adoption of the password vaults was mostly observed among the people of 26-30 years old. Students that pursue a career in computer engineering are the majority of the password manager users, while the students of social sciences are prevailing among the respondents that had no prior knowledge related to the application. The tendency was observed that the majority of respondents that claim to have advanced computer skills, use password managers, whilst the respondents with basic computer knowledge were not aware of password vaults. Further studies could be focused on investigating the demographic factors as mediating in addition to the theoretical models.

4.5.2 Technology Characteristics and Task Characteristics

As the outcome of the research, it can be concluded that technology characteristics have significant effect on the task technology fit (TTF), whereas task characteristics did not show any statistical significance in explaining TTF. Moreover, the indirect relationship shows that technology characteristics not only influences task technology fit, but subsequently it affects behavioral intentions to use password managers, and eventually the adoption ($p<0,01$). Furthermore, since TTF affects adoption directly, the technology characteristics affect adoption through TTF. Meanwhile, task characteristics were not proven to be significant in explaining TTF or adoption.

It may be concluded that the users are more likely to use the software if the functionality of it seems attractive. Even if the tasks would need a password manager, it does not mean that the user is likely to use the software. There are many alternative ways to manage passwords, so if an individual does not find the technological characteristics appealing, it is highly unlikely that the decision will be made to adopt the software. The security and usability limitations of password vaults may seriously affect the further adoption of the software. Furthermore, it is possible that some individuals were not aware of the useful and important features of password vaults. The study shows that in case the students find password managers to be technologically suitable,

they are likely to be willing to use the software. However, it is important to present the technological advantages of vaults in order to make them attractive. A study conducted by Fagan et al (2017) shows similar results: some of the participants of the research claim that they do not use password managers due to lack of usability.

4.5.3 Social Influence

Social influence showed statistical significance in explaining behavioral intentions in the context of password managers. Moreover, Social Influence is significant in explaining Adoption indirectly through BI. This means that if the close relatives, friends or people from other social circles are using password managers, it is more likely for the individual to consider adopting the password vaults. As the study was done regarding the students in Europe, it may mean that if the fellow students are using password managers, it is more likely for the individual to start using the software as well. This leads to the conclusion that word of mouth is an important factor for password vaults to become attractive among students. The study conducted by Maclean and Ophoff (2019) shows that social influence is not significant in explaining behavioural intentions. However, the target group for the research was different.

4.5.4 Effort Expectancy

Effort Expectancy is not significant in explaining the adoption of password managers. However, indirectly through Performance Expectancy and Behavioural Intentions, Effort Expectancy is significant in explaining password manager adoption. It means that a student is likely to adopt a password manager if the software seems to be easy to install and performs well according to the needs. The findings match the study of Maclean and Ophoff (2019), though this thesis research not only analyzed the direct effect of effort expectancy over behavioural intentions, but also indirect effect on adoption of password managers.

4.5.5 Facilitating Conditions

Facilitating conditions were also important in determining the adoption factor. If the students consider the facilities provided to them as suitable for using password managers, they are more likely to use password managers. The study by Maclean and Ophoff (2019) shows that facilitating conditions are not significant in explaining

behavioral intentions, which matches this thesis study. However, the relationship between facilitating conditions and adoption was proven by this research.

4.5.6 Performance Expectancy

Performance expectancy was proven to be one of the most important factors in forming behavioral intentions towards the adoption of password managers. This finding matches the results mentioned by Maclean and Ophoff (2019). If the students in Europe see that the software is useful and is capable of effectively completing the required tasks, then they are more likely to be in favor of adopting it. Furthermore, the study by Fagan et al (2017) proves that respondents avoid adopting password managers if they see lack of need and usability drawbacks. However, the participants of the study by Fagan et al (2017) who use password managers, reported the convenience and usefulness of the software.

4.6 Practical Implications

Based on the study, if a company providing password managers should focus on ensuring that the services are convenient, secure and user-friendly. The emphasis should be done on providing potential users with the necessary knowledge on the usefulness of password managers, as well as the technological benefits of the software. This may be achieved through marketing campaigns, for example. Moreover, social influence should not be underestimated. It is important to understand that the close family and friends' opinion have a serious impact on the intentions of the individuals to use password managers in the future.

The study may be used to create trainings targeting the factors that may lead to password managers adoption among students. This way the students could develop secure practices in terms of managing their credentials, which could be beneficial for their own security, as well as the security of the companies that are further employing the graduates. The model used in the study was proven to be suitable for studies related to password manager adoption.

The study included collecting demographic information, which was not eventually studied in-depth. The next step of the research would be to analyze whether gender, age,

or educational background has an influence on the decision whether to adopt the software. Moreover, the online experience, as well as the experience with using the Internet may be a mediating factor in the model. The future research could focus on investigating the correlation between the demographic information and the adoption among the individuals towards password managers. Moreover, the study did not include the data collected through the open question regarding the reasons for the individuals that led to them not adopting password managers.

4.7 Future Directions

In order to confirm the factors affecting the adoption of password managers, a future suggestion would be to study the adoption of the password managers in-depth, by first presenting the software including a more detailed information on the functionality and the benefits of it, and later collecting the responses from the same group of people after they get familiarized with the product. This way it could be possible to verify whether the behavioral intentions lead to the adoption of the software within the same group of respondents.

The demographic review points to the assumption that there is a correlation between the number of accounts used daily and the adoption of the password managers. Furthermore, there is a possibility that the educational background and the level of education influence the decision on whether to adopt the use of password vaults. For example, the majority of the current users of password managers study computer science, while most of the respondents who reported not being knowledgeable about the software study social sciences. There is a possibility that there is a correlation, hence it would be beneficial to verify whether the demographic factors could be mediating in forming the behavioral intention to adopt the software, or these factors could lead directly to adoption of password vaults. This may help understand which groups of students should be targeted in terms of security trainings and additional studies on security practices. A separate study may be conducted in the future among the students with a non-technical background in order to confirm which factors to focus on in order to encourage the adoption of password manager. Furthermore, an emphasis may be done on how students from different countries react towards the software, which could

help in creation targeted trainings tailored to the specifics of the background of the users.

With the increasing amount of services available online, it is very important not to underestimate the impact of poor password management on the security of sensitive data. If credentials are stolen or hacked, the attacker may gain access to banking details, healthcare information, personal details shared on social media, or even corporate data, if the job-related accounts are compromised. The study was conducted among students since it is important to understand how to enforce best practices related to online security among the people that will later be employed and will have to deal not only with their personal data but also the data related to their workplace, which may be highly confidential. There are, however, some limitations in this study, since it was not possible to profoundly examine the responses in relation to the demographical background. However, this can be a subject for further study. Moreover, the research confirms that the combination of TTF and UTAUT could serve for the statistical analysis related to the adoption of password managers.

5 Conclusion

Passwords are a common way of authentication for different types of accounts. People use passwords to log in to their online bank, healthcare systems, study, and work-related portals. Since the capacity of human memory is limited, many people reuse the same passwords for different websites, or they create simple passwords to remember them easily. This causes a serious security risk. If a hacker is able to steal a password, all the sensitive information will be stolen. Password managers were created to facilitate secure password management; however, many people decide not to use the software for managing their credentials. The study is aiming at finding out what are the factors affecting password manager adoption among students in Europe. The research questions were the following:

1. What is a demographic profile of a European student who (does not) use a password manager?
2. What factors affect password manager adoption among the European students?

This research was conducted in order to answer the aforementioned questions with the help of UTAUT and TTF models. These models have been successfully used in other studies related to the adoption of various technologies among different demographic groups of people. The variations of UTAUT and TTF models were brought together for the customized model that was further used as the framework for this thesis.

The study was conducted with the use of a survey that consisted of questions that presented the items that formed various variables taken from UTAUT and TTF models. The data sample consisted of 265 valid responses. Smart-PLS tool was used for the statistical analysis, as it was suitable for non-normal data distribution.

It was found that a person who is a male of 26 – 30 years old, studying Master's in computer engineering is more likely to use password manager. On the other hand, a female of 21-25 years old, doing a Master's in Social Sciences fits the profile of a non-

user. This can help target the training to raise awareness about a secure way of managing passwords.

The outcomes of the study show that the main factors affecting behavioural intentions among students in Europe are performance expectancy and social influence. Furthermore, task technology fit, behavioural intentions and facilitating conditions affect adoption directly, whereas performance expectancy, effort expectancy, technology characteristics and social influence affect adoption indirectly. The respondents are more likely to use password managers if it suits their needs for regularly performed tasks. Moreover, a positive feedback from close social circles may affect password manager adoption among European students. The perceived effort and the suitable facilities were also proven to be important factors leading to the adoption of password managers.

References

Arias-Cabarcos, P., Marin, A., Palacios, D., Almenarez, F., & Diaz-Sanchez, D. (2016). Comparing Password Management Software: Toward Usable and Secure Enterprise Authentication. *IT Professional*, *18*(5), 34-40. doi: 10.1109/mitp.2016.81

Aurigemma, S., Mattson, T., & Leonard, L. (2017). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications?. *Proceedings Of The 50Th Hawaii International Conference On System Sciences (2017)*. doi: 10.24251/hicss.2017.490

Bojan, V. (2017). *Security Evaluation of Password Manager Browser Extensions* (Graduate). Aalto University.

Bozorgkhou, N. (2015). An internet shopping user adoption model using an integrated TTF and UTAUT: Evidence from Iranian consumers. *Management Science Letters*, *5*(2), 199-204. doi: 10.5267/j.msl.2014.12.017

Boukayoua, F., De Decker, B., & Naessens, V. (2014). A keyboard that manages your passwords in Android. *2014 International Conference On Privacy And Security In Mobile Systems (PRISMS)*. doi: 10.1109/prisms.2014.6970592

Brostoff, S., & Sasse, M. (2000). Are Passfaces More Usable Than Passwords? A Field Trial Investigation. *People And Computers XIV — Usability Or Else!*, 405-424. doi: 10.1007/978-1-4471-0515-2_27

Casey, T., & Wilson-Evered, E. (2012). Predicting uptake of technology innovations in online family dispute resolution services: An application and extension of the UTAUT. *Computers In Human Behavior*, 28(6), 2034-2045. doi: 10.1016/j.chb.2012.05.022

Charoen, D., Raman, M., & Olfman, L. (2007). Improving End User Behaviour in Password Utilization: An Action Research Initiative. *Systemic Practice And Action Research*, *21*(1), 55-72. doi: 10.1007/s11213-007-9082-4

Chiasson, S., & Oorschot, P. (2006). *A Usability Study and Critique of Two Password Managers*. Carleton University.

Chinchor, N., Cook, K., & Scholtz, J. (2012). Building Adoption of Visual Analytics Software. In *Expanding the Frontiers of Visual Analytics and Visualization*. https://doi.org/10.1007/978-1-4471-2804-5_29

Daradkeh, M. (2019). Visual Analytics Adoption in Business Enterprises. *International Journal Of Information Systems In The Service Sector*, *11*(1), 68-89. doi: 10.4018/ijisss.2019010105

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319. doi: 10.2307/249008

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior Ever Follows Intention?. *Proceedings Of The 2016 CHI Conference On Human Factors In Computing Systems - CHI '16*. doi: 10.1145/2858036.2858265

Englert, B., & Shah, P. (2009). On the design and implementation of a secure online password vault. *Proceedings Of The 2009 International Conference On Hybrid Information Technology - ICHIT '09*. doi: 10.1145/1644993.1645063

Fagan, M., Albayram, Y., Khan, M., & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-Centric Computing And Information Sciences*, *7*(1). doi: 10.1186/s13673-017-0093-6

Ferratt, T. W., & Vlahos, G. E. (1998). An investigation of task-technology fit for managers in Greece and the US. *European Journal of Information Systems*. https://doi.org/10.1057/palgrave.ejis.3000288

Fukumitsu, M., Hasegawa, S., Iwazaki, J., Sakai, M., & Takahashi, D. (2016). A Proposal of a Password Manager Satisfying Security and Usability by Using the Secret Sharing and a Personal Server. *2016 IEEE 30Th International Conference On Advanced Information Networking And Applications (AINA)*. doi: 10.1109/aina.2016.45

Gebauer, J., Shaw, M., & Gribbins, M. (2010). Task-Technology Fit for Mobile Information Systems. *Journal Of Information Technology*, *25*(3), 259-272. doi: 10.1057/jit.2010.10

Golrang, M. (2013). *CredProxy: A Password Manager for Online Authentication Environments*(Graduate). University of Ottawa.

Goodhue, D., & Thompson, R. (1995). Task-Technology Fit and Individual Performance. *MIS Quarterly*, *19*(2), 213. doi: 10.2307/249689

Hair, J., Hult, G., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Los Angeles: SAGE.

Hoque, R., & Sorwar, G. (2017). Understanding factors influencing the adoption of mHealth by the elderly: An extension of the UTAUT model. *International Journal Of Medical Informatics*, *101*, 75-84. doi: 10.1016/j.ijmedinf.2017.02.002

Karole, A., Saxena, N., & Christin, N. (2011). A Comparative Usability Evaluation of Traditional Password Managers. *Information Security And Cryptology - ICISC 2010*, 233-251. doi: 10.1007/978-3-642-24209-0_16

Li, H., & Evans, D. (2017). *Horcrux: A Password Manager for Paranoids*. University of Virginia.

Maclean, R., & Ophoff, J. (2019). Determining key factors that lead to the adoption of password managers. *2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018*. https://doi.org/10.1109/ICONIC.2018.8601223

McCarney, D., Barrera, D., Clark, J., Chiasson, S., & van Oorschot, P. (2012). Tapas: design, implementation, and usability evaluation of a password manager. *Proceedings Of The 28Th Annual Computer Security Applications Conference On - ACSAC '12*. doi: 10.1145/2420950.2420964

Magsamen-Conrad, K., Upadhyaya, S., Joa, C., & Dowd, J. (2015). Bridging the divide: Using UTAUT to predict multigenerational tablet adoption practices. *Computers In Human Behavior*, *50*, 186-196. doi: 10.1016/j.chb.2015.03.032

Miller, G. (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review*, *63*(2), 81-97. doi: 10.1037/h0043158

Negahban, A., & Chung, C. (2014). Discovering determinants of users perception of mobile device functionality fit. *Computers In Human Behavior*, *35*, 75-84. doi: 10.1016/j.chb.2014.02.020

Nightingale, A. (2009). A guide to systematic literature reviews. *Surgery (Oxford)*, *27*(9), 381-384. doi: 10.1016/j.mpsur.2009.07.005

Oliveira, T., Faria, M., Thomas, M., & Popovič, A. (2014). Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. *International Journal Of Information Management*, *34*(5), 689-703. doi: 10.1016/j.ijinfomgt.2014.06.004

Schougaard, D., Dragoni, N., & Spognardi, A. (2016). Evaluation of Professional Cloud Password Management Tools. *Current Trends In Web Engineering*, 16-28. doi: 10.1007/978-3-319-46963-8_2

Stobert, E., & Biddle, R. (2014). A Password Manager that Doesn't Remember Passwords. *Proceedings Of The 2014 Workshop On New Security Paradigms Workshop - NSPW '14*. doi: 10.1145/2683467.2683471

Tannen, R., Jackson, K., & Temple, J. (2019). *Evaluating and Improving the User Interface for Password Management Software – A Case Study*. Camegie Mellon University.

Ting, G., & Deng, Y. (2012). A study on users' acceptance behavior to mobile e-books application based on UTAUT model. *2012 IEEE International Conference On Computer Science And Automation Engineering*. doi: 10.1109/icsess.2012.6269483

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425. doi: 10.2307/30036540

Yang, B., Chu, H., Li, G., Petrovic, S., & Busch, C. (2014). Cloud Password Manager Using Privacy-Preserved Biometrics. *2014 IEEE International Conference On Cloud Engineering*. doi: 10.1109/ic2e.2014.91

Yadegaridehkordi, E., Iahad, N., & Ahmad, N. (2014). Task-technology fit and user adoption of cloud-based collaborative learning technologies. *2014 International Conference On Computer And Information Sciences (ICCOINS)*. doi: 10.1109/iccoins.2014.6868439

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2010.01.013

Zigurs, I., & Buckland, B. (1998). A Theory of Task/Technology Fit and Group Support Systems Effectiveness. *MIS Quarterly*, *22*(3), 313. doi: 10.2307/249668

Zobayer, A., Kader, A., Ur Rashid, M., & Nurunnabi, M. (2019). User perception of mobile banking adoption: an integrated TTF-UTAUT model. *Journal Of Internet Banking And Commerce*, *22*(3), 1-19.

Appendix A.

Table I. Demographic distribution: password manager users and non-users (frequency)

Distribution	Users	Non-users
Gender		
Female	19	144
Male	41	57
N/a	1	3
Age		
18-20	5	24
21-25	20	108
26-30	23	51
31-35	6	14
Over 35	7	7
Education level		
Bachelor's	24	93
Master's	30	97
PhD	7	14
Educational background		
Law	1	5
Computer Engineering	18	13
Economics	6	38
Education	2	9
Humanities	5	27
Medicine	9	10
Natural Sciences	9	15
Social Sciences	6	50
Other Engineering	1	10
Other	4	27
Amount of passwords used		
None	1	8
Less than 5	10	82
Less than 10	30	91
10 to 15	15	20
More than 15	5	3
Computer proficiency level		
Basic	3	45
Intermediate	23	119
Advanced	35	40

Table II. Items used for the research

Item Code	Item Description	Source
TaskC1	I need to manage my passwords anytime anywhere	Oliveira et al, 2014
TaskC2	I need to operate my accounts anytime anywhere	Oliveira et al, 2014
TaskC3	I need to access my accounts several times a day	Oliveira et al, 2014
TaskC4	I use different passwords for different accounts	Self-generated
TaskC5	I use strong passwords (containing alphabets, numbers and characters) for my accounts	Self-generated
TaskC6	I need to remember passwords for my accounts	Self-generated
TaskC7	I need to write down passwords somewhere safe	Self-generated
TC1	With password management software I can access my accounts anytime anywhere	Self-generated
TC2	Password management software provides a real-time service	Oliveira et al, 2014
TC3	Password management software provides secure services	Oliveira et al, 2014
TC4	Password management software provides a quick service	Oliveira et al, 2014
TTF1	Password management software is appropriate for managing my passwords	Oliveira et al, 2014
TTF2	In general, password management software meets my password management needs	Self-generated
TTF3	In general, password management software is enough for password management	Oliveira et al, 2014
TTF4	Using password management software does not fit with my practice preferences	Self-generated, reverse-coded
EE1	Learning to use password management software is/will be easy	Oliveira et al, 2014
EE2	It is/will be easy to enter in the password management software interface	Oliveira et al, 2014

Table II (Continued). Items used for the research

EE3	It is/will be easy to use the password management software skillfully	Oliveira et al, 2014
EE4	I do not/will not have any doubts about what I am doing when I am using the service	Oliveira et al, 2014
SI1	The people that influence me value the use of password management software	Oliveira et al, 2014
SI2	The people that influence me use password management software	Oliveira et al, 2014
SI3	Those people that influence my behavior think I should use password management software	Venkatesh et al, 2003
SI4	Those people that are important to me think that I should use password management software	Venkatesh et al, 2003
SI5	The people that influence me help me learning about password management software	Self-generated
SI6	The people that influence me introduce me to password management software	Self-generated
SI7	At my school/university I have been introduced to use of password management software	Self-generated
PE1	I feel password management software is/will be useful	Self-generated
PE2	Password management software brings/will bring convenience to password management	Self-generated
PE3	Password management software lets/will let me access my accounts quickly	Oliveira et al, 2014
PE4	I save/will save time by using password management software	Self-generated
PE5	Password management software optimizes/will optimize operations related to my accounts	Oliveira et al, 2014

Table II (Continued). Items used for the research

FC1	I have all the necessary resources towards using password management software	Oliveira et al, 2014
FC2	I have the necessary know-how towards using password management software	Oliveira et al, 2014
FC3	If I have any difficulty using password management software, I do have a support to help me	Oliveira et al, 2014
BI1	I have the intention of managing my passwords by using the password management software	Oliveira et al, 2014
BI2	I'm curious about password management software	Oliveira et al, 2014
BI3	I have the intention of managing my accounts using a password management software	Oliveira et al, 2014
BI4	I have the intention of logging in with the help of a password management software	Oliveira et al, 2014
BI5	I plan to use a password management software	Oliveira et al, 2014
Adopt1	I use password management software	Oliveira et al, 2014
Adopt2	I use password management software to manage my passwords	Oliveira et al, 2014
Adopt3	I use password management software for logging to various systems/accounts	Oliveira et al, 2014
Adopt4	I subscribe to products that are exclusive to password management software	Oliveira et al, 2014

Table III. Statistical Values of Items

	Mean	Median	Min	Max	Standard Deviation	Excess Kurtosis	Skewness
EE1	3,962	4	1	5	0,885	0,529	-0,78
EE2	3,819	4	1	5	0,906	0,127	-0,523
EE3	3,721	4	1	5	0,901	0,113	-0,507
EE4	3,223	3	1	5	1,088	-0,639	-0,134
SI1	2,747	3	1	5	1,085	-0,592	0,107
SI2	2,623	3	1	5	1,195	-0,805	0,215
SI3	2,649	3	1	5	1,185	-0,794	0,202
SI4	2,449	2	1	5	1,135	-0,687	0,313
SI5	2,26	2	1	5	1,124	-0,715	0,45
SI6	2,272	2	1	5	1,229	-0,756	0,573
SI7	1,638	1	1	5	1,015	1,77	1,601
FC1	3,426	4	1	5	1,23	-0,787	-0,405
FC2	3,411	4	1	5	1,216	-0,758	-0,437
FC3	3,17	3	1	5	1,158	-0,703	-0,204
BI1	2,977	3	1	5	1,291	-1,1	-0,042
BI2	3,475	4	1	5	1,179	-0,446	-0,56
BI3	3,045	3	1	5	1,288	-1,057	-0,074
B4	3,026	3	1	5	1,287	-1,104	-0,049
BI5	2,989	3	1	5	1,333	-1,162	-0,027
PE1	3,706	4	1	5	1,055	-0,114	-0,629
PE2	3,785	4	1	5	1	0,336	-0,743
P3	3,796	4	1	5	0,992	-0,017	-0,56
PE4	3,611	4	1	5	1,128	-0,556	-0,462
PE5	3,442	3	1	5	1,034	-0,261	-0,285
TaskC1	3,555	4	1	5	1,218	-0,697	-0,518
TaskC2	3,917	4	1	5	1,078	-0,066	-0,851
TaskC3	4,185	4	1	5	0,967	1,073	-1,209
TaskC4	3,83	4	1	5	1,231	-0,75	-0,674
TaskC5	4,211	4	1	5	0,968	0,864	-1,189
TaskC6	3,981	4	1	5	1,151	0,219	-1,024
TaskC7	2,857	3	1	5	1,423	-1,321	0,152
TC1	3,645	4	1	5	1,036	-0,393	-0,352
TC2	3,642	4	1	5	0,95	-0,227	-0,318
TC3	3,404	3	1	5	0,951	-0,234	-0,172
TC4	3,664	4	1	5	0,901	-0,284	-0,219
TTF1	3,6	4	1	5	0,997	-0,639	-0,186
TTF2	3,46	3	1	5	1,078	-0,617	-0,197
TTF3	3,449	3	1	5	1,049	-0,549	-0,17
TTF4	3,234	3	1	5	1,181	-0,917	-0,158

Table III (Continued). Statistical Values of Items

Adopt1	2,102	1	1	5	1,53	-0,599	1,017
Adopt2	2,125	1	1	5	1,518	-0,6	0,998
Adopt3	2,132	1	1	5	1,508	-0,565	1,003
Adopt4	1,551	1	1	5	0,902	1,255	1,476