LUND UNIVERSITY
School of Economics and Management
Department of Informatics

Password Managers in a Home Computer Environment

Bachelor Thesis 15 HEC, course SYSK16 in Informatics

Authors: Emil Björk
Pontus Pieslinger

Supervisor: Miranda Kajtazi

Correcting Teacher: Odd Sten

Password Managers in a Home Computer Environment

AUTHORS: Emil Björk and Pontus Pieslinger

PUBLISHED: Department of informatics, Lund School of Economics and Management, Lund University

PRESENTED: May, 2020

FORMAL EXAMINOR: Christina Keller, Professor

DOCUMENT TYPE: Bachelor Thesis

NUMBER OF PAGES: 46

KEY WORDS: Information Systems, Information Technology, Unified Theory of Acceptance and Use of Technology, Diffusion of Innovation, Password Manager.

ABSTRACT (MAX. 200 WORDS):

Passwords are one of the most used tools for authentication. Because of this, password managers have been developed to allow for increased protection and usability when managing passwords. However, the research of password managers in the context of usability coupled with diffusion of technology is unclear. Thus, the study's purpose is to investigate how usability influences management of and the motivation to use PMs diffused among users. This is done by analysing data using the key concepts of usability and diffusion of technology via the theoretical models Unified Theory of Acceptance and Use of Technology and Diffusion of Innovation. The study is based on a survey with 120 respondents, where the focus has been to investigate the relationship between the key concept to gather descriptive statistical data using multiple choice questions. It is found that individuals preferred including numbers instead of capital letters or special symbols in their passwords. Furthermore, it is also concluded that home computer users value ease of use over protection in the usability-security trade off in password managers. Following these findings, the study suggests that the focus of password managers should lie on usability to gain recognition among users.

Content

Figures

Tables

Key words

This thesis uses several keywords that are shortened as acronyms and therefore are placed here, along with a definition that this thesis follows.

Acronym	**Keyword**	**Definition**
IS	Information Systems	System designed to collect, process, store and distribute information (Marakas & O'Brien, 2005).
IT	Information Technology	Technology designed to collect, process, store and distribute information (Turban, 2008).
UTAUT	Unified Theory of Acceptance and Use of Technology	Theory that aims to clarify users' intentions by using an IS and its usability (Venkatesh et al., 2003).
DOI	Diffusion of Innovation.	Theory that explains the acceptance by society of innovation over time (Rogers, 1995).
PM	Password Manager.	A software used to create, encrypt, manage and store passwords (Techopedia, 2020).

1 Introduction

Information security has experienced rapid development over the past five decades. What started off as a joke between colleagues in the 1960s has rapidly escalated to the huge global issue it is today. To tackle these issues, a standard means of protection was developed, requiring a password to access sensitive or personal information. This later developed into more modern flexible security systems such as password managers (PMs), face recognition and fingerprint scanners to name a few. These systems displayed a theoretical view of how the concepts usability and security with regards to IT can be efficiently used to increase user friendly protection. When a data breach occurs today, companies take it very seriously and do their utmost to prevent it from happening again by hauling in third-party investigators, notify regulators and provide free credit monitoring for any impacted customer (Osborne, 2019). However, cyber issues have evolved into an individual problem, implying that individuals should consider signing up for cyber security services as well.

Information Technology (IT) is known to help companies efficiently obtain resource management and plan amongst fields such as strategic competitive advantage to maintain said advantage in the market (Mata et al., 1995). When IT was first introduced to the world, companies quickly realised the potential with including it in their organisations. However, with the globalization that later came as a result of IT's upbringing, it became evident that the present Information Systems that existed were required to go through a development process in order to become Global Information Systems, which are more suited to handle the implication of the modern world (Porter, 1990). Globalization also helped smaller companies, especially family companies, and other firms that are managed from home and not necessarily an office. With sudden new uprising phenomena, such as IT, there tends to be underlying issues in the system itself that needs recognition. However, the problem needs to be highlighted for such recognition to take place which is why cyber security was developed.

Passwords are widely used on various online platforms as means of authentication. For example, in relation to subscription fees, shopping etc. This has created an increased concern about identity theft. Gaw & Felten (2006) support this statement and suggest that this problem is further strengthened from the fact that people tend to reuse the same password over different applications. This results in increased security risk, as one breach potentially opens doors to a multitude of other breaches (Gaw & Felten, 2006). In their study consisting of 49 undergraduates, they conclude that these users tend to have three or less passwords that they reuse at least twice.
As time goes by it is normal to pile up more accounts across platforms. However, the study shows that this does not increase the number of passwords created. Meaning that the amount of accumulated accounts does not go hand in hand with higher password variance (Gaw & Felten, 2006).

In their study Gaw & Felten (2006) also discovered flaws in users' security awareness in terms of what could be a potential threat. While they were quick to identify that some personal information is best kept out of passwords such as pet names, social security number etc. This type of information is oftentimes something stalkers can discover if they want to and by that start to experiment with potential breakthroughs. This fact also applies to people you consider close to you, as they by default often have a lot of personal information that they can use (Gaw & Felten, 2006). Furthermore, respondents to their research ranked people close to

them as the biggest threats to them. Respondents also had a hard time thinking about non-human attackers (Gaw & Felten, 2006).

As was found in the study by Tam et al. (2010), users are aware of what the characteristic differences between a good and bad password are as well as what password management practices to avoid. It was also found in the same study that what motivates users to engage in bad password management behaviour is lack of immediate consequences and the convenience-security trade off. Furthermore, the research continues explaining that the relationship between the intention to pick a secure password and password quality was much weaker than the relationship between the security-convenience trade off and password quality. This suggests that despite the increased technological advances, humans remain the weakest link in password management (Tam et al., 2010). However, given the innovative ways of a technology such as password management, it poses the question whether the research by Tam et al. (2010) is still accurate.

The past few years have seen a dramatic increase in the number of data breaches of major corporations and government agencies and that number only continues to grow. These significant breaches make it now more important than ever to find new ways to access private data (Bachman, 2014). Previous research has shown that human interaction is the weakest link when dealing with security in IT (Bulgurcu et al., 2010; Tam et al., 2010; Mackie & Yildrim, 2019). Thus, by minimizing human interaction with the system we also minimize potential security breaches. This thesis aims to investigate how home computer users perceive password managers as a safer way of password management through diffusion of technology and its usability.

1.1 Research Problem

Security within IT poses continuous challenges for businesses. Not only do they have to keep up on an organizational level, they also must make sure employees are on the same page. Furthermore, research has in fact shown that Employees tend to be the weak link in the equation (Bulgurcu et al., 2010). Statistics have shown that more than one in four IT related risks can be pointed towards insiders (PwC, 2014).

Due to the employee being a potential weak link in a company's IT security, it shows how an individual can impact a company's security today, even in big corporate businesses. Seeing as people handle security poorly as an employee, is there really anything stopping these employees to do the same thing in their private life. Bachmann (2014) means that usage of a password is one of the most common ways of getting access and authorization. He also states in the same source how traditional password security will be less relevant in the near future. With this information in mind, it paves the way for new technology in the field, making passwords a focal point of identity verification for such technology on a multitude of platforms today. Due to the innovative nature of technologies such as PMs and the issues of potential security breaches that password management technology faces, the next step in the development process of passwords should be considered. From a diffusion of technology point of view, password managers have gained momentum particularly in the last decade (Anderson and Agarwal et al., 2010; Liang et al., 2019; Bachmann, 2014). We found that there are many studies that discuss security and threats as an overall subject (Moody et al., 2018), but oftentimes focus on the corporate side of things, tackling home computer users in

terms of password managers only superficially (Fatokun et al. 2019). Most research in the field of passwords tends to focus on usability alone from an organizational perspective (Bulgurcu et al., 2010), with few managing to tackle usability from a home computer user side of things (Anderson and Agarwal et al., 2010; Liang et al., 2019; Bachmann, 2014). But the absence of research about usability coupled with the diffusion of technology in recent times allows research to open a new avenue to tackle usability with the expansion of technology. In general, security concerning PMs from a home computer user's point of view sparked an interest in investigating the connection between how people manage their passwords in their daily life and how that type of management can be improved.

1.2 Research Question

What effect does usability coupled with diffusion of technology have on home computer users of password managers?

1.3 Research Purpose

The problem proposed in the thesis suggests that IT-security is a vulnerable area to most businesses. By default, that is a vulnerability to individuals. However, we found that most research in the area tends to focus on how these threats can pose danger to larger organisations and not the home computer users. How to make people create a secure password. Therefore, we consider that the diffusion of technology as a subject to address home computer users' usage of PMs is lacking in the matter (Anderson and Agarwal et al., 2010; Liang et al., 2019; Bachmann, 2014).

To be able to pose a threat you need to be able to gain authorization or access in one way or another. To do so you often need to verify, and one of the most used tools to do so is a password (Bachmann, 2014). Technologies such as multi-factor authentication and password management software have been hailed as ultimate solutions to the password problem. Such conventional wisdom has been challenged by recent events. For instance, reports found that nine popular password managers were affected by critical vulnerabilities that expose user credentials (Wei, 2017). In other words, using password management software containing complex passwords could lead to a higher security risk in comparison to using non-managed passwords. The thesis purpose is to investigate how home computer users manage their passwords regarding usability coupled with diffusion of technology in the current context. Investigating this allows the study to derive how usability influences management of and the motivation to use PMs diffused among users. This is investigated in two ways. First, we investigate how the usability of passwords is handled. For example, the usage of letters and numbers. Secondly, we investigate the aspect of diffusion of technology regarding PMs. Are people willing to use a PM? If not, why are they unwilling to do so?

1.4 Limitations

Our research aims to investigate how the home computing space handles passwords, in other words how the individual handles them. Thus, the aim is not to look further into how this is translated into individuals' professional lives but might prove upon correlation between the two.

The respondents of the survey have a large representation from young adults (age 18-25). This is probably influenced by the survey spread, which was over multiple platforms where young students are gathered. This is not necessarily negative, but it must be taken into consideration when analysing the data collected. It has the possibility to skew the data, but ultimately it allows for analysis over how a user manages their passwords.

Throughout the research different terminology has been discovered regarding PMs. Password management systems are also a term that was found. PMs are the term that focuses on the technology side of things, while password management system refers to specific systems. In the thesis PMs have been chosen as the main usage. However, when the research started out and we created the survey, the term of password management systems seemed more fitting at the time due to it being deemed a more familiar term.

1.5 Potential Stakeholders

Every person that consumes any online platform, website or anything alike would benefit in some way from taking part in this study. Not only does it shed light on areas regarding how passwords are handled in general and how they can pose a threat to your online presence, but also how that can affect you directly. By identifying how home computer users deal with the handling of passwords, this could be of interest for employers to investigate as well. If a lot of individuals have a poor way of managing their personal passwords, what would stop them from integrating that into their professional life?

2 Theoretical Framework

2.1 Information security

Information security is a central part of password management. Passwords serve as the bank vault lock of today's crucial information and to handle this responsibility in a respectable manner, products such as password managers have been developed. It is widely accepted that in IT security today that the human factor is deemed the weakest link (Bulgurcu et al., 2010). Manual password creation and human memory is often the fault of not having access to information in a system, stating the suggestion that IT systems today are better off with as little human contact as possible.

The designing of software systems to train individuals in information usage is one example of such a measure, organisations adopting a user-oriented approach to the design of modern computer systems is another (Preece et al., 1994).

IT serves as a simplification of information handling due to its bigger capacity and solid protection, being a big leap forward in the field of information security. Issues regarding malware and viruses are new problems that have come along with it, leading into the field of cyber security. The fields of information security and cyber security are often seen as interchangeable, however cyber security also includes protection of the individual as well as information security as argued by von Solms & van Nierkerk (2013). With the cyber-attack developing as a threat due to new IT, additional ethical problems arise since society as a whole in the aspect of information systems potentially could be attacked digitally (Dayem, 2018), putting more emphasis on the importance of cyber security. This shows how information security has evolved into something that affects the individual, not only organisations.

The password and user id combination has been an efficient way to share secret information between a digital system and a user for many years as stated by Conklin et al. (2004). The one dependent attribute in this relation is the human cognitive ability to remember the log-in information. As Conklin et al. describes in their research how this initially worked well on a small scale with few users but eventually turned out to be problematic due to globalization and newer technology increasing the number of users and systems. The user is now tasked with remembering multiple passwords and systems, which becomes increasingly difficult. To tackle this newfound problem, users developed software to store user information and thus creating a connection between otherwise isolated systems. Conklin et al. also describes how this connection influences system level security. A good example of such a system is today's password managers.

It is commonly known within systems science that user input can affect the system operation. However, when this is applied to the interconnected systems of today the definition of the system span becomes vague. Some systems today include multiple other systems through interconnected transactions, meaning that the potential breach in one system due to poor password authentication can affect other connected systems as well (Conklin et al., 2004).

Despite the problems with interconnected systems, the influence of said systems have kept growing. This growth in combination with the limits of human cognitive ability has caused

systems to be intertwined with each other in unpredicted ways. In 2002 the Slammer Worm attack exploited this weakness, with 75 000 confirmed infections it infected more than 90 % of vulnerable hosts within 10 minutes, doubling its size every 8.5 seconds (Moore et al., 2003).

2.1.1 Password Security

Passwords are one of the most used mechanisms for allowing access to different types of systems. This puts large emphasis on issues regarding passwords for lots of people around the globe daily. Despite this assumption there has been some disagreements around the subject, where some have claimed that traditional password security will be less relevant in the near future (Bachmann, 2014). Nonetheless, little evidence has been shown to prove this so far. Larger organizations that are forced by law to implement enhanced security have shown struggles to move past passwords for securing access to various systems (Cimpanu, 2018). Additionally, it has often been the case that solutions to solve this dilemma have resulted in unintended consequences instead.

Enforcing certain policies for example, may force the user to use a password they find too complex. By doing this they may feel the need to write down the password on a piece of paper, or in a note on their smartphone. Ultimately, this somewhat kills the initial purpose of the enforced policy - to create a secure password. Cazier & Medlin (2006) further presents issues regarding passwords. People tend to use memorable things to create their idea for passwords, whether it would be pet name, name of child, anniversary dates etc. These are areas which could easily be explored and used within systems to crack passwords, which potentially further speed up the process of cracking the password.

Mackie & Yildirim (2019) present in their study how passwords rarely are limited by technical issues, rather are they limited by the human memory. Therefore, they propose a user-friendly framework to set up passwords. This includes persuasive messages that inspire the users to craft a memorable text password. By doing so, less burden is put on the human memory to remember various passwords. Thus, authentication via passwords involves an interplay between usability of human computer interaction and level of security, however this relationship has proven difficult to manage due to the incompatibility of the two. This has been further confirmed via Mackie & Yildrim (2019) who found in their study that the creation of a long password gives you a secure password but makes you more likely to forget it.

The result of Mackie & Yildrim (2019) research shows that users given guidelines rather than strict rules, tend to create stronger passwords. It is also indicated that these people often remember their passwords better. This provides evidence that it is worthwhile to create guidelines for users at the password creation screen. However, the participants of the research complied with being part of a research, meaning that this might not represent how things play out in real life. To tackle this problem, it could be an idea to enforce a mandatory guideline section before you ultimately create the password itself (Mackie & Yildirim, 2019).

Hashim et al. (2010) present data that supports angles of the study made by Mackie & Yildirim (2019). More specifically on how to communicate to the user through messages or feedback on how to improve the security of their password. The password strength meter is a tool used by many websites. Simply put, this tool calculates the strength of the password and

then displays for the user via different visual effects how strong their password is perceived. This can be through a bar that fills up, or coloured text (Hashim et al., 2010). This method has been shown to increase the security, but the effectiveness of the strength meter has been a topic of discussion. Its presence does not remove the usage of poor passwords. Furthermore, it is presented that fear appeals can be an efficient way to manipulate behaviour. This can be used in addition to a strength meter and by displaying certain messages to the user, make them think twice before executing on their password. This could for example be displaying password as weak with a red font, adding information about how long it would take to crack the password assuming the attacker could execute x amount of attempts every second (Hashim et al., 2010).

2.1.2 Password Managers

Password managers are software applications that can be used to store and manage different passwords that the user has. This allows for a smoother process in terms of taking care of the user passwords. This system will keep track of the passwords for various online websites, making the online presence easier for the user. Generally seen, this type of system can be monitored from a so-called master password. Currently, the market offers many different types of password managers, varying on different factors such as how they store information and how information is encrypted. The password details can for example be stored and encrypted on the local memory or in the cloud, before it gets auto filled into a form (Techopedia, 2020).

Other solutions also exist. Such as portable password managers downloaded on a mobile device. Which in other words can be used as an authenticator. Allowing a user to maintain various passwords on different software add up to create a safer online profile for the user. Password managers can also be a great way to protect yourself from other malicious attacks such as keylogging etc (Techopedia, 2020).

2.2 Theoretical Perspectives in Action

There are numerous studies that tackle security and passwords as such. Oftentimes this is aimed towards a corporate perspective. However there seems to be a lack of studies that takes home computers as a subject in the matter (Anderson & Agarwal, 2010; Chen & Zahedi, 2016). While some of the research is applicable to both areas, there are things that would be interesting to investigate from a home computer perspective.
Anderson & Agarwal (2010) present in their study how home computer users are affected by cybersecurity. There are three main questions they tackle;

What are the factors influencing a home computer user's security behaviour?

Are there differences in the factors influencing a home computer user's intentions to protect her own computer versus the internet?

Can the strength of some of these factors be changed through message cues?

Even though the study is somewhat old, we found that it is hard to get newer studies that

tackle similar areas of research (Chen & Zahedi, 2016). The study by Liang et al., (2019) also takes the individual's approach and highlights previous research that tackles individuals alone, without bringing in the research from the employee's perspective on security that has been popular over the years. Bulgurcu et al (2010) and Moody et al. (2018) are two important examples of that. However, in Liang et al. (2019) it becomes evident that focusing on internet home computer users as such, Andersson and Agarwal (2010) are exceptional. They stress the fact that large corporations invest in infrastructure that helps keeping computer assets secured. However, as a home computer user you are left entirely on your own. This means that you as a home computer user is a lot more exposed, since home computer users represent a large portion of units included in the infrastructure of cybersecurity (Anderson & Agarwal, 2010).

Anderson & Agarwal (2010) focus on two different aspects. The behavioural intentions to secure your own computer along with the behavioural intentions to secure the internet. These two aspects are theorized to be driven by three determinants.

1. Attitudes toward security related behaviour
2. Psychological ownership of the relevant object
3. Social influence in the form of subjective and descriptive norm

They further connect this to how humans behave to stay healthy. Most humans wash their hands multiple times a day. They do so to keep potential bacteria, viruses, or anything alike away. By doing this not only do they keep them away from themselves, they indirectly keep it from spreading to other human beings (Anderson & Agarwal, 2010). However, protecting your own computer might be a more natural behaviour. Afterall it is a physical object that you possess and sometimes even own. Protecting the internet though, can be a little trickier. The internet is not a physical object that humans can own per say. They merely connect to a network where they can interact with others and solve problems in various ways. Therefore, it is not completely out of hand to say that the protection of the internet along with protecting other humans from illnesses happens subconsciously (Anderson & Agarwal, 2010).

Anderson & Agarwal (2010) present results that hint towards the combination of cognitive, social-, and psychosocial components as major building blocks when it comes to influencing home computers security behaviour. The user's intentions can be enhanced by message manipulations made prominent to the user. Messages that focus on positive feedback have shown to be more effective than negative ones. Furthermore, they stress the importance of specification regarding what is being the security object, since people's security behaviour varies a lot between objects. Suggesting that some objects are treated with higher security than others (Anderson & Agarwal, 2010).

Liang et al (2019) present in their paper how individuals deal with IT security threats, taking the perspectives of problem- and emotional focus. They refer to this as problem-focused-coping (PFC) and emotion-focused-coping (EFC). While PFC has been researched extensively in the past, they see lack of research in the field of EFC. EFC impacts PFC in both a competitive and supportive manner. If a user takes more EFC action, this lessens the chance for rational decisions taken by PFC and vice versa (Liang et al 2019). Further they present two different types of EFC, inwards and outwards. Inwards EFC refers to behaviours such as psychological distancing, wishful thinking and denial. Psychological distancing is particularly dangerous, as it creates a distraction that takes away from attention identifying IT threats. The

latter two focus on cognitive change, as it changes the perception of IT threats, either by making them bigger than what they are or by downplaying them. This matches up well with the study from Anderson & Agarwal (2010), as they also found cognitive components to be important when investigating home computer influence on security behaviour. Outward EFC refers to behaviours such as searching for emotional support and venting. In other words, seeking sympathy and understanding from people in one's social network (Liang et al., 2019).

It appears that both PFC and EFC are utilized when dealing with IT security threats. EFC mostly acts as a modifier in relation to PFC. In the paper they conclude that inwards EFC leads to a faulty adaptation, because it lowers the quality of a user's PFC. Outward EFC on the other hand, has shown some indication of increasing the PFC of users. Seeing as they search for other people's point of view (Liang et al., 2019).

To further increase our understanding of password security and how its adversity effects usability as a concept, we also investigate Chen and Zahedi (2016) who delves into the cultural importance of cyber-security. By investigating the differences between the nations USA and China, the study provided the field of password security with essential information on how different cultural groups tackle the issue of security threats. Chen and Zahedi developed a context-sensitive model to study online security behaviours for this purpose, which evidently indicated the significant moderated influence of the nation and the pervasive impacts of individual differences.

Fatokun et al. (2019) investigate further into security behaviour of students at a Malaysian university. More specifically they focus on how age, gender and educational level may influence user’s security behaviour. They conclude that all three in some way impact the security behaviour. In doing so, they put these factors in relation to numerous obstacles to explore how this may impact the security behaviour. Examples of obstacles would be familiarity with cyber-threats, cues to action, peer behaviour, perceived vulnerability etc. Worth noting is that both age and gender yielded more statistical important data than educational level. This could hint to the fact that educational level might not correlate with security behaviour. Furthermore, it is found that security self-efficacy, computer skills and prior experience are all factors that are impacted by gender (Fatokun et al., 2019).

Fatokun et al. (2019) also investigated how the age of student’s impact security related issues, such as hacking incidents. They discovered that the effect was higher in terms of perceived severity on older students as opposed to younger. The study is concluded with a clear statement that cyber security training would be beneficial to students and therefore, it would be great for institutions to establish a framework for enabling this training. Doing this would increase the amount of home computer users, increasing the importance of research in the field. Furthermore Fatokun et al. (2019) present what factors would be interesting to investigate in future research. There amongst, cultural background, academic performance, health habits etc (Fatokun et al., 2019).

Below are some statistics provided to shed light on how the online portfolio for the entire world looks today.

According to Statista (2020) as of January 2020, the world has:

4.54 billion active internet users

4.18 billion unique mobile internet users

3.80 billion active social media users

3.75 billion active mobile social media users

To add these numbers on top of each other in combination with the thought that most people use numerous platforms daily, it becomes apparent that there are multiple billions of passwords floating around. Therefore, management of passwords should be taken very seriously from the world's population.

Study on Home Computer Users	**Focus**	**Concepts**	**Field Study**	**Key Findings**
Liang et al. (2019)	How individuals cope with security issues, problem- and emotion focused	Usability	Study 1: Experiment Study 2: survey	Problems and emotions interplay and effect each other
Andersson & Agarwal (2010)	How home computer users are affected by cybersecurity	Usability, Diffusion of technology	Study 1: Questionnaire, Survey Study 2: Qualitative, Interviews	Cognitive factors impact security behaviour
Moody et al. (2018)	Creating a better understanding of security policy compliance	Usability	Revising previous theories	Similarities between different ISS models from an individual's perspective
Chen & Zahedi (2016)	Context sensitivity of user's online security perceptions and behaviours to national and individual attributes	Usability	Survey, Observations	Cultural perception impacts the severity of security threats
Fatokun et al. (2019)	Age, gender and educational impact on security behaviour	Usability, Diffusion of technology	Questionnaire, 340 students	Security training is necessary, Age and gender seemingly have higher influence

Table 1. Summarizing previous research in the field.

2.3 Introducing the Theoretical Lenses

To understand how passwords are used from a user perspective, there are theoretical lenses that can help to give that understanding. To clarify the role of home computers in PMs the study aims to tackle both usability and diffusion of technology as two central concepts. On one hand, a study by Venkatesh et al. (2003) has shown that the Unified Theory of Acceptance and Use of Technology (UTAUT) model presents usability as a central concept to understand how certain technologies are used by users from any angle: home-computer users, employees, children at schools, etc. On the other hand, a study by Everette M. Rogers (1995) shows that the Diffusion of Innovation (DOI) model uses innovation as a central concept that explains the adoption of an idea from a technological point of view. Identifying these two studies helped us to explain and better understand the two theories described below. The study then follows with a proposal for a view on how passwords can be studied, where two concepts driven from these theoretical explanations are put in relationship.

To further explain the position of this study in relation to the two theories (UTAUT and DOI) the intention is to better understand how their concepts can be applied in the aspect of password management from a home user perspective. Doing that, the application of the theory as such is not considered in the study, but rather the use of its key concepts that are explained further below.

2.3.1 Unified Theory of Acceptance and Use of Technology (UTAUT)

The model used in the investigation is Unified Theory of Acceptance and Use of Technology (UTAUT) which delves deeper into the underlying reasons why only certain technology is perceived as usable by the user. It's based on behavioural intentions and uses independent factors as stated in Theories Used in IS Research Wiki (2015): Performance expectancy, Effort expectancy, Social influence, Facilitating conditions, Gender, Age, Experience, Voluntariness of use.

Venkatesh et al. (2003) reflect on data in their paper User Acceptance of IT. From tables 5 and 6 in their paper, they found seven different constructs that had an impact on users' intentions with IT. From these seven they decided upon four of which would have an impact on usage behaviour and acceptance.

Constructs being following:
Performance Expectancy, Effort Expectancy, Social Influence and Facilitating Conditions

Additionally, each of these constructs get influenced from the key moderators of the figure. Key moderators being following:

Gender, Age, Experience and Voluntariness of Use.

Down below you can find the visual representation of the result in Figure 1 - The model of UTAUT.

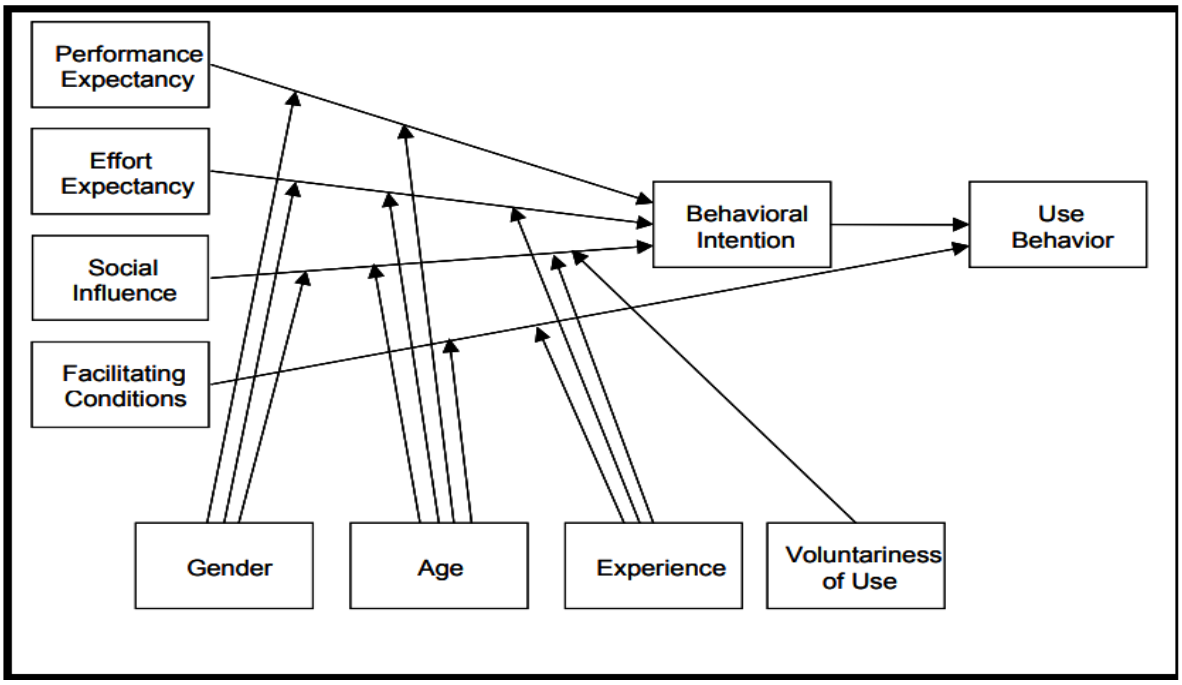

Figure 1. Research Model - UTAUT

Performance expectancy takes into consideration how the individual feels about using a system. This includes expectancies such as finishing work faster, increased productivity, increased effectiveness, or an easier time to reach the goal (Venkatesh et al., 2003). It is also the sole construct that takes into account the intentions of the person using the system, allowing the model to include definitions about user anticipation of the system regarding identified areas such as the ones used by Venkatesh et al (2003) in their study.

Effort expectancy is to what degree individuals have ease with getting to know a system. This can involve multiple different factors such as learning the system, understanding the system, is the system hard or easy to understand etc (Venkatesh et al., 2003).

Social influence reflects upon how important an individual feels it is for them to use a system. With the perspective from other individuals. In other words - does other individuals find it important that I use the system. This importance can be enforced from many different angles. It might be the management that promotes the usage of the system. Might as well be co-workers that use the system and find them valuable, hence why they want to encourage the rest of the organization to use it. It can also be the individual themselves putting value into a system. Other people within the organization with prestigious positions might use them which can make other individuals interested in a system (Venkatesh et al., 2003).

Facilitating Conditions refers to what degree an individual believes the technical- and organizational infrastructure support the overall usage of certain systems. This could for example be in the form of instructions and guidance being available for the individual. It could also be in terms of a support-unit being available to assist if an individual encounters difficulty with the system (Venkatesh et al., 2003).

Venkatesh et al. (2003) present a few ideas for future coming research in the field. Specifically, they want further research to focus on identifying new constructs that potentially could further increase the knowledge of behaviour from users in different systems. They also

reveal that it might be a hard task to complete. Giving UTAUT currently explains up towards 70 percent of the variance in intention and therefore the ceiling might be within reach (Venkatesh et al. 2003).

2.3.2 Diffusion of Innovation Theory (DOI)

Diffusion regarding innovation is defined in this theory as the process by which an innovation is communicated through certain channels over time (Rogers, 1995). Individuals are having different degrees of willingness to adopt innovations, because of this it is accepted on general terms that the total amount of individuals who accept an innovation are normally distributed over time. This theory originates in how a certain phenomenon gains momentum over time (Rogers, 1995). In the research regarding the usability of home computer users' management of PMs, DOI is used to explain innovation from a diffusion of technology point of view.

Adopting a new idea comes with many challenges, innovation in many cases requires a substantial amount of time to be processed, potentially adopted and merged into organisations and society. DOI refers to the process by which individuals adopt a new idea or phenomenon, in his book Diffusion of Innovations (1995) Rogers describes how this process functions. He describes the continuum of innovativeness as partitioned into five adopter categories, these are described in Figure 2 below as innovators, early adopters, early majority, late majority and laggards. The dominant attributes of each category are defined for innovators as venturesome, early adopters as respect, early majority as deliberate, late majority as sceptical and laggards as traditional (Rogers, 1995). Figure 2 below represents the five adopter categories and the percentage of adopted individuals.

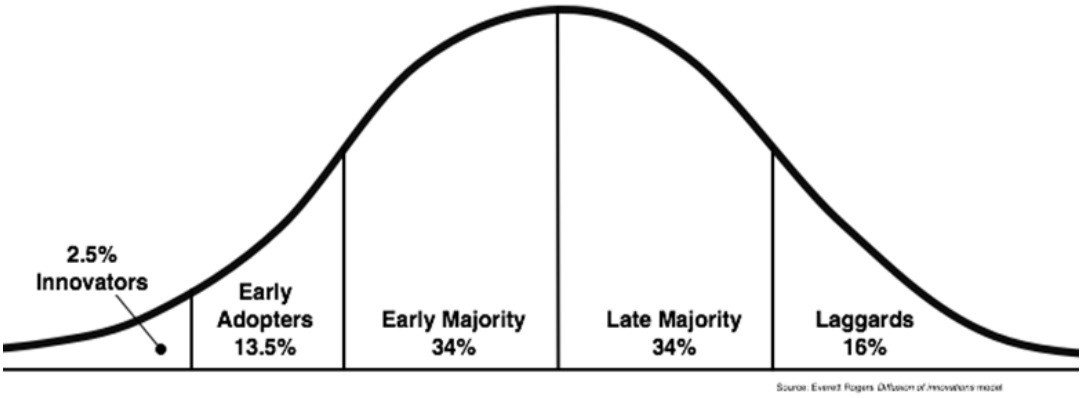

Figure 2. Diffusion of Innovation Theoretical Model

Since individuals are different and we view opportunity subjectively, initially there are a limited number of individuals or social groups that are willing to adopt a new idea and are defined as the *Innovators* and *Early Adopters*.

Present data has shown that *innovators* are the first to adopt because the individuals who identify with this group require a shorter innovation decision period compared to others. This is because the Innovators have more favourable attitudes toward new ideas, meaning that the interest in new ideas overrides the resistance to change (Rogers, 1995). Innovators as a group of individuals receive a lot of scepticism because of their change-oriented nature and new thinking. In a traditional society this is most evident since the innovators seldom serve as opinion leaders but instead more like creative new-thinkers, however in a more modern

society that is accustomed to change and is more receptive to change or alteration they receive less such scepticism. Deriving from this it can be concluded that the systems norms determine whether opinion leaders are innovators (Rogers, 1995). The more accepted innovators are in society the more power will be granted these individuals and thus more innovation will be present.

Early Adopters spread the word regarding the newfound idea and based on their opinions the next group of individuals who then form an opinionated understanding of this and decides whether to adopt the idea. Earlier adopters have a greater ability to deal with abstractions than later adopters. Innovators must have the ability to adopt a new idea based on an abstract stimuli. Compared to the early adopters, later adopters such as the early or late majority can wait and observe the development of the innovation before adopting and thus are not required to have the ability to deal with abstractions (Rogers, 1995).

The *Early Majority* are welcoming to new ideas and adopt them slightly faster than the average person. They play an important role between the early- and late majority. They provide synergy between the different networks of the system. As a part of the early majority it is common for individuals to initially show scepticism, but eventually end up adopting the new idea. The goal is to not be the one taking on the risk of trying out new ideas. On the other hand, there is also a fear of being left behind and being last on adopting new ideas and innovations (Rogers, 1995).

The *Late Majority* is relatively slow to adopt new ideas. They tend to do so slightly slower than the average member of society. Reasons they finally adopt may be caused by increasing network pressure. Innovations are faced with a sceptical view, and as a late majority it is often common to be among the last ones in the social circle to adopt a new way of thinking. The utility an innovation can bring gives interest, but pressure from peers is a necessary step to adopt the new way of thinking. For a late majority it is important to miss out on any potential uncertainty. In other words, they want to make sure risks are eliminated, so that it is safe to adopt the new idea (Rogers, 1995).

Laggards are the last individuals to adopt a new idea. These individuals are commonly very resistant to change and traditional by nature. Without strong acceptance by society these people will resist the change by any means necessary because of their belief that things are handled in a perfect manner and that change only will result in more problems and confusion. These people usually see things through a narrower and more simplistic short-term viewpoint. They serve as the opposite end of the spectrum compared to the innovators, slowing down innovation. Together, they create a balance of the concept of innovation.

2.4 Theoretical perspective development

Given the theoretical models UTAUT and DOI there is an understanding that from a password management perspective, concepts of usability in password management and innovation in password management are highlighted. First, usability becomes important because UTAUT itself shows “use” as a dependent factor that is most interesting to grasp how it’s applied in reality. Secondly, from an innovative point of view as represented in DOI, it is observed that in recent years password protection is key among security experts. This emphasizes the importance of innovating new ways of increased protection. Putting

innovation into the context of diffusion of technology allows us to view new ways of developing already existing technology. The relationship of these two concepts shows the capability for an interesting and a different view of how password management is viewed among home computer users.

In table 2 below data is shown to present the different theoretical perspectives used in the research and furthermore specifies what concepts and areas this is applicable to.

Theoretical Perspective	**Concepts**	**Applicability**
UTAUT	Usability of PMs	Password creation Password usage Password sustain
DOI	Diffusion of PMs	Face recognition Fingerprint scanner

Table 2. Theoretical Model Applicability

The combination of DOI and UTAUT made way for the creation of our own model. This model features the interplay between usability and diffusion of technology in terms of innovation with password management as the binding factor between the two. After carefully analysing both theoretical models, the relationship between diffusion of technology and usability becomes evident. Password security is a concept that is based on human interaction, passwords are created and remembered by human cognitive ability, putting usability at the centre of the concept. Due to password security and management having to do with usability in such a way, it makes the field compatible with the theory of UTAUT, who's main purpose is to define user behaviour. Similarly, the theory of DOI proposes innovation as adoption over time, making it applicable to a field that is still in early development such as PMs. Due to password managers being a relatively new technology, there are still new or existing system features in development. Suggesting that usability has a direct impact on user acceptance, this theoretical research model discusses to what extent the relationship between usability and innovation in terms of diffusion of technology influences password management.

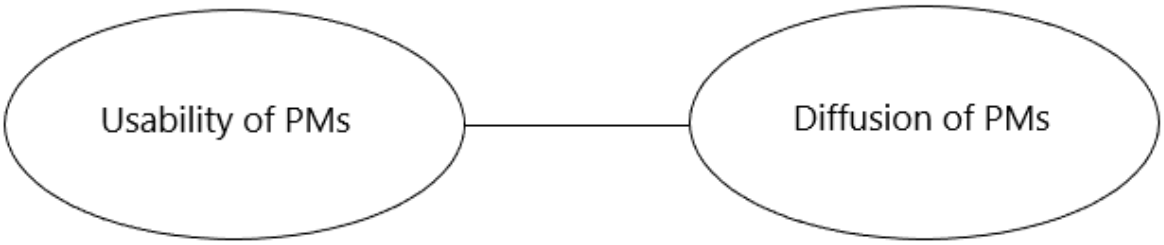

Figure 3. Composed Research Model.

The interesting interplay here is how passwords continuously interact with both concepts to take passwords to the next stage. Hashim et al. (2010) has specified different ways innovation

has pushed users in a certain direction in terms of usability. This includes using fear of simplicity and strength meters for passwords.

Agarwal and Prasad (2007) investigated the paradoxical relationship between investment in IT and gains in productivity and found that it has been classified as a lack of user acceptance of IT innovations. This study aims to narrow this research to entail password security and management more specifically. Attempts at predicting user acceptance of new IT innovations have been made in the past. These attempts found that the individual characteristics and attributes of the invention was a recurring theme of user acceptance, as was found in Agarwal and Prasad's study (2007). Furthermore, in the same study it was concluded that individual characteristics of an IT innovation in fact explains acceptance behaviour and that the characteristics required for different acceptance outcomes differ. Comparing this concept with password management will allow a better understanding of user acceptance within this field.

3 Research Methodology

3.1 Research Approach

The research is of quantitative nature where the questions will be based in a survey method. The choice of quantitative method is a result of the broader perspective it provides. The field of password security on an individual level is easier to derive knowledge from using this method given the vastness of the web and the data collected. With a quantitative approach we can capture a wider picture of the presented problem and research question by targeting a larger number of home computer users. From a critical point of view, while we cannot get in-depth views on how they interact with their online world and how they keep themselves secure, we spread the understanding on a broader level to many such users. This more general information on user interaction coupled with diffusion of technology also serves as a functional basis for a broader cultural community since the study is not limited to users from one area. In the study of Chen and Zahedi (2016), it was found that cyber-security was directly impacted by culture. Given the fact that home computer users exist globally, gathering information from individuals from different cultures provides less biased data which further shows the applicability of a quantitative research approach for this study. While in our study we don't tackle cultural perspectives, and we neither expend it on cross-culture, we still argue that a home-computer user from one cultural perspective might bring new and interesting results on how technology diffused into society and how it increases usability of PMs.

The numbers of respondents spiked quickly, but also went down rather rapidly. Hence why we shut the survey down after five days. First 24 hours of the survey, we received about 75% of respondents. Meaning that the coming five days only represented 25% of total respondents. There were additional ways of further spreading the survey, however the cost-benefit ratio of these spreads was not deemed as valuable enough to include in the survey. The decision was made that the number of respondents gathered was enough for creating a credible in-depth analysis of the collected data. The survey was shut down at roughly 120 respondents, which correspond well with the numbers of answers we needed per question.

3.2 Towards the empirical development of the survey

The idea behind the survey is to collectively summarize questions that can allude to what effect usability coupled with diffusion of technology have on home computer users. First and foremost, there are overview questions such as age, gender etc.

The introducing section is targeted towards usability of passwords from a broader perspective. By collecting this data, it allows us to see how the home computer user interacts with their passwords. The purpose of the questions in this section is to help create an understanding of how the user views security in contrast to passwords, creating a deeper connection with usability. By investigating user behaviour when creating or managing passwords it creates an understanding of why people use or refrain from using password managing tools, additionally it also provides context regarding choice of password manager. This is where the model of UTAUT is represented in the survey. It explains usability and behavioural patterns of

individuals, allowing the survey to ask questions regarding typical user behaviour when creating or managing security passwords. Furthermore, this allows us to analyse an individual's choice of password regarding consistency, validity and protection level from a usability point of view.

Furthermore, the survey investigates how diffusion of technology, which serves as our definition of innovation in the given context, interplays with passwords. This is done using the DOI model, which explains innovation over time and some key concepts that individuals find attractive and unique. Investigating this concept will allow us to identify traits of preferred innovative PMs. Here, existing PMs are presented and asked upon, providing detailed information vital for the investigation. By asking questions in the survey regarding what the user finds intriguing in using specific PMs, it clarifies why the respondent is using the PM. Innovation in this regard plays a key role in PMs due to it still being a new phenomenon, much more so than in already established fields who are no longer in the initial establishment phase. The DOI model explains the innovative stage of products, by analysing the respondent's choice of password manager the model helps deducing what makes each one more attractive to the user. This may be due to the popularity of a system, or the influence of other factors such as an individual's workplace. If a password manager has been used related to work and it has shown to be a valuable tool, the user might see value in integrating it into its personal life.

The final section of the survey revolves around identifying what different password managers the respondents are familiar with or have had any experience using. The respondents get to choose from 13 different options in a list. Those 13 password managers have been identified by researching online platforms such as TechRadar for most used PMs. The PMs that were mentioned and reviewed multiple times on these platforms were included in the survey.

3.3 Survey development

The survey is developed based on an interplay between two theoretical concepts that have been identified as crucial in our study to tackle password management from a home user perspective.

In doing so, we have extracted key concepts of the two theories as presented in Table 3 below. The survey questions are developed based on the applicability of these concepts in an actual context, which is that of home computer users and their password management strategies. In the table down below, it is shown what theory tackles what area. Additionally, it is shown which questions in the survey that represent these areas of research.

Concepts	Applicability	Survey Questions
Usability of PMs	Password creation Password usage	Q3-Q9
Diffusion of PMs	Password Manager Diffusion in terms of fingerprint and/or face recognition technology Password Manager Usage	Q10-Q14

Table 3. Survey Question's Relationship with Theoretical Models

3.4 Selection of Participants

The survey used to conduct the research was spread through social media, both through public posts and direct messages on platforms such as Facebook, Discord, WhatsApp and Instagram. We also spread the survey in social media groups on named platforms, where people share surveys and trade answers. This way various thesis writers could help each other out by answering each other's survey. Engaging in direct messages to familiar faces allowed the survey to be spread further, acquiring a wider spread which allowed for an increased number of respondents. The study's aim is selective in its targeting of a young audience due to their higher technological competence. This was done intentionally to make the collected data more credible regarding PMs. Fatokun et al. (2019) influenced this approach by showing that the effect of impact security related issues was higher in terms of perceived severity on older students as opposed to younger, showing the relationship between age and security technology.

3.5 Data Analysis Approach

Descriptive statistics is the main key of data analysis for this study. Ultimately, the goal is to find correlations between different descriptive statistics. This allows us to find areas of interplay where usability is coupled with diffusion of technology. It also allows us to highlight data deemed more vital for the research, creating a better understanding of context. To do this, the findings of our survey are put into figures, visually displaying the information collected. These will be divided into three subheadings as can be found in the research section. First, two individual perspectives will be presented, tackling usability of technology and diffusion of technology. Moving forward, a third perspective will be presented, tackling diffusion of technology as an influence on usability. Dividing the work like this creates better understanding of context, allows for critical analysis, interpretation of figures and attempts to find rationale behind the emergence of main findings.

3.6 Ethics

Before the survey itself started, an initial screen giving some basic information about the survey and us as writers were given. For example, we attend Lund university, studying informatics. It was also clarified that the data gathered from this survey would serve as material for our bachelor thesis and nothing else. Contact details were given so that respondents had the opportunity to get in touch with us in case they had any further questions or thoughts.

Furthermore, numerous questions throughout the survey include the option of answering "other". The respondents are asked kindly to specify what it is they refer to, which provides the study with data that would have otherwise been lost. However, this was decided to be non-mandatory so that respondents would not feel forced to submit uncomfortable data. The respondents were kept anonymous for the survey.

3.7 Research Quality

The definition of some of the options given as possible answers to the included questions are to a certain degree subjective, meaning that there is no exact definition regarding some of the answer alternatives provided in the survey, examples of answer alternatives that fit this description are *often* or *sometimes*. Using such options limits the survey's result accuracy regarding PMs and constricts the depth potential of the data analysis.

It later became evident that some answer alternatives that were provided for the questions in the survey were too vague, creating unnecessary confusion for the respondent. This is the case in question 11 as shown by Figure 15 in Appendix B, where the answer latest technology was provided alongside with more specific recent technology such as face recognition and two-factor authentication.

Looking at the survey in hindsight, the latter parts could be structured in a better way to allow more interesting data. When comparing Q10 and Q12, it seemed as though respondents during the survey was aware that they used a password manager, that being Google Chrome's built-in function. The idea of first including a question regarding if they use a password manager with a yes or no answer, with a follow up question about whether they use Google Chrome's function for remembering passwords. This could provide some insight into how home computer users view password managers, and how they are present in their everyday life without really being noticed too much.

3.8 Characteristics of Respondents

We did not emphasize many characteristic questions within the survey. The two questions presented involved gender and age of the respondent. Initially the vast majority was male respondents, something that made us think twice about why. This also made us try to target audiences with females to restore a balance. However, when the survey closed, there was no real shocking difference in gender amongst respondents. Genders were distributed by; 50% male, 45% female and 5% other.

Age is where large differences can be found within respondents, over 50% are between the ages of 18-25. Furthermore, about 30% are between ages 26-35. This might be a result of where the survey was spread. The Facebook groups were mostly consisting of students, hence why the overwhelming numbers in the lower age brackets. This may affect the survey result in some way. Fatokun et al. (2019) declare that both age and gender are factors that affect security behaviour, further strengthening the idea that perceived severity by security threats increases with age.

4 Research Findings

In this chapter the data collected from the survey are compiled. In the appendix you can find the detailed tables and diagrams connected to the findings from the survey.

4.1 In Context to Usability of Technology

The survey consisted of seven questions that are directly connected to the concept of usability derived from UTAUT. From these it is possible to extract how user behaviour tends to be regarding how management of passwords are handled from a home computer user perspective.

The first question about usability tackles the amount of characters contained in the respondents' passwords. There are numerous sources citing different amounts of characters needed for a password to be considered secure. However, it is always a combination of other factors. In the survey we decided to go with the alternatives of less than nine, or more than nine. From this we can conclude that about 65% of respondents use passwords with nine or more characters, and about 35% use a password consisting of less than nine characters. A clear majority uses more than nine. But still there are quite a few users settling for rather short passwords. In terms of how home computer users vary their passwords across different applications, the respondents show very little effort in the matter. Well over 60% says that the very same password often occurs. While about 7% claim that they always use one specific password for each consecutive application. Appendix B, Figure 7 & 8 show these findings.

The survey also concluded that home computer users tend to keep the same versions of their password for extended periods of time. Around 7% say they are always switching up their password, in a way that it is not matching any older password that they have used in the past. The remainders of respondents either never change password to match older versions, sometimes do it or often. Appendix B, Figure 9 shows these findings.

Out of all respondents, less than 1% say they do not contain numerical numbers in their password, ie. 1-9. Showing that this is a well adopted concept to integrate in their security behaviour. However, there are other areas that prove to be less well adopted concepts for home computer users. About 20% of respondents say they always add special symbols when creating a password. Special symbols refer to the likes of ;, !, @, ?, etc. The largest part of respondents said they sometimes do this, about 40%. While little less than 30% say they never use special symbols in connection to their passwords. Appendix B, Figure 10 & 11 show these findings.

The next question tackles whether home computer users involve upper- and lower casing. The results here show that this concept is well perceived. Only 1.5% or respondents confirm they never involve upper- and lower casing. Leaving a whopping 98.5% to either sometimes, often or always integrating this method. The last question focuses on if respondents tend to use the same password for both personal- and professional use. The numbers reveal that little less than 40% never use the same password for both purposes. That leaves about 60% of respondents to a group where they sometimes integrate passwords in both their professional- and personal life. Appendix B, Figure 12 & 13 show these findings.

In the table below is the data summarized regarding the questions related to usability. The numbers are a bit more accurate but rounded to closest 0.5%.

Survey question	**Response - in terms of % (rounded numbers)**
Q3. How many characters do you tend to use in your password?	< 9 - 35% > 9 - 65%
Q4. Are you using different passwords for different applications?	Always different - 7.5% Often different - 29.5% Same often occur - 63%
Q5. Do you often switch your passwords not to match the older version that you've used?	Never - 28.5% Sometimes - 56.5% Often - 7.5% Always - 7.5%
Q6. Does your password contain numbers?	Yes - 99% No - 1%
Q7. Does your password contain special symbols? (!, @, % etc.)	Never - 27% Sometimes - 41 % Often - 11% Always - 21%
Q8. Does your password involve both upper- and lower casing?	Never - 1.5% Sometimes - 28.5% Often - 22% Always - 48%
Q9. Do you often use the same passwords for your professional- and personal life?	Never - 38% Sometimes - 28.5% Often - 20% Always - 13.5%

Table 4. Descriptive Statistics of Survey Answer on General Password-related Questions on Usability

4.2 In Context to Diffusion of Technology

The survey contains five additional questions that involve how diffusion of technology in recent years may have an impact on password management. The aim with these questions is to investigate how home computer users manage their passwords and to conclude if they use any additional tools for assistance. Along with what they find convincing about a password management system, in terms of what it offers as a service. Worth noting is that these questions were put as non-mandatory in the survey. Meaning that a respondent could leave the field empty in case they did not utilize a password manager or have any input about what they find valuable to look for in a password manager.

The first question asks what password manager the respondent is using to help manage their passwords. Worth noting is that 70 out of 119 responded on this question, which indicates that quite a few people don't utilize the usage of a PM. Out of these 70 respondents, 49 said they use the built in function that Google Chrome offers. Meaning that whenever a user logs into an application through the Google Chrome browser, they have the option to save the password and use it for further logins. Additionally, there were quite a few that responded under the "Other" section and gave other similar answers. Such as built in functions in Mozilla, Safari etc. The other most prominent password manager was LastPass, receiving 6 votes. Through the other section there were also 5 people mentioning that they use KeePass, making that the second most used password management system out of the third-party software. Appendix B, Figure 14 shows these findings.

The next question in the survey concludes what factors makes it intriguing for the home computer user to use a password management system. There was an even distribution between different factors, but with one outlier. Ease of use/flexibility racked up around 60% of the votes, making it a clear favourite. Second highest was accessibility, which gained about 26%. The other alternatives all hoover around 15-20%. Appendix B, Figure 15 shows these findings.

Some of the respondents interpreted the next question wrong, or rather it got confused for being the same question as a previous question (Q10). These questions are listed below;

Do you use a password management system to help you manage your passwords? If yes, which ones:

What password management system do you focus on when it comes to helping you manage your passwords?

However, an interesting finding here was that more people answered on the latter question and even more people gave the response of Google Chrome built in function. Appendix B, Figure 16 shows these findings.

When asked about what makes a password manager to stand out from others available in the market. Respondents were mostly agreeing on what they look for. Latest technology, popularity, influence by the workplace and others, were all sitting around the 10% mark. While the clear favourite was ease of use, racking up little less than 80%. This shows somewhat similar patterns to Q11, but ultimately here people saw ease of use as a more important factor. Appendix B, Figure 15 shows these findings.

Survey question	**Response - in terms of % (rounded numbers)**
Q10. Do you use a password management system to help you manage your passwords? If yes, which ones:	Google Chrome (built in) - 70% Dashlane - 1.5% LastPass - 8.5% 1Password - 1.5% RoboForm - 0% Other - 24.5%
Q11. What makes it intriguing for you to use a certain type of password manager that is different from the rest?	Latest Technology (Fingerprints etc) - 18.5% Face recognition - 12.5% Two-factor authentication - 20.5% Ease of use/flexibility - 61% Accessibility - 26.5% Other - 11.5%
Q12. What password management system do you focus on when it comes to helping you manage your passwords?	Google Chrome (built in) - 67.5% Dashlane - 2.5% LastPass - 6.5% 1Password - 1.5% RoboForm - 0% Other - 24%
Q13. If you use any password management system, what makes it stand out from the rest of systems that are available to you?	Latest technology in authentication - 6.5% Ease of use - 78.5% Popularity - 10.5% Influenced by workplace - 8% Other - 9.5%
Q14. Are you familiar or use any of the following password managers?	Look at Figure 18 in appendix B.

Table 5. Descriptive Statistics of Answers to the Survey on Password-related Questions on Usability.

4.3 In Context to Diffusion of Technology as an Influence to Usability

Two important questions in the survey that seem to correlate and support one another are represented in Q12 and Q13. The data summarized from the respondents about these questions can be found in the Figure 4 below. The picture on top in the figure focuses on what PMs respondents focus on in managing their password, while the bottom picture represents what makes certain PMs stand out from others. A lot of respondents focus on Google Chrome's PMs. As stated before, given answers under *other* were aimed towards different browser PMs such as Mozilla, Safari etc. Suggesting that even more respondents focus on built-in options. This fact matches up well with the amount of answers claiming that ease of use is the main thing that makes a PMs stand out from others.

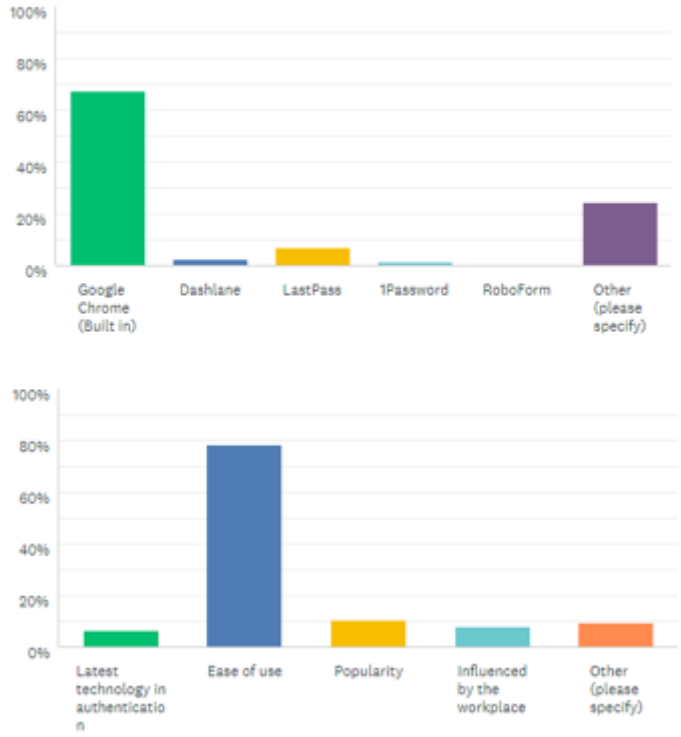

Figure 4.

This is a challenging aspect for non-built-in PMs since they are not as easily accessible. For such PMs to gain recognition it requires more substantial research than already integrated PMs. This research includes decisions regarding which PM is preferable in terms of security, manual installation, popularity etc. All these factors naturally go against the most preferable trait which was found to be ease of use in the study. This shows that home computer users tend to not go for the option that provides the best security, but rather the one that makes them feel secure and require less effort.

5 Discussion of Results

Gathering the responses on password managers, there is a tendency among the home-computer users that have responded to the survey to show that they will most likely use a strong password, such as using more than 9 characters with a combination of upper- and lower casing letters and numbers. But, at the same time, the analysis shows that the majority prefer to use the same combination of passwords for many different applications. From a research point of view, this shows a great vulnerability since malicious attacks are sophisticated to decipher even strong passwords. It also strengthens the deduction that passwords are limited by the human mind (Mackie & Yildirim 2019). Using the same password in multiple security systems creates an easier way into the entanglement of information which is the web of interconnected systems (Conklin et al., 2004).

As is found in the survey, individuals tend to move towards password simplicity in password construction. When the majority (63%) of home computer users claim that they would rather use the same password for different applications, it shows that the majority refrain from complex tasks and progress towards simpler tasks, such as ease of use or flexibility. This is highlighted by the data samples collected from question 4 and question 11 in the survey, as is shown in Figure 8 and 15 in Appendix B. This derives that usability and diffusion of technology within password management have a clear connection to ease of use, proposing that people prefer simplicity over more complex security at the expense of increased risk. This is supported by the study made by Bulgurcu et al. (2010), in which they found employees to be the weakest link when working with security, meaning that they pose the biggest threat to businesses by their security behaviour.

Emphasizing on the ease of usability and the flexibility sought after in password managers, Google chrome was chosen as the main password manager. The parallel between these have become clear through the survey, given the ease of use majority in Figure 15 (61%) and 17 (78.5%) and the selection of chrome as the most used password manager in Figure 16, Appendix B. Due to its built in feature, Google Chrome's password manager is easy to use and accessible. It presents itself to the user, regardless if the add-on is called upon or not, making it an easy choice of password manager.

Given that what peaks the individual's interest in a system is ease of use as was deducted in the previous paragraph, there are not many systems matching these criteria. This clear difference between the view of user and creator of a system shows the complication of creating a password manager that is deemed innovative and usable. Since there is a clear correlation between usability and ease of use it complicates the focus of innovation, shifting it from increasing security and protection to making the system easy to use and flexible. By taking this approach it is inevitable that systems are developed with flaws. This is strengthened by previous research (Agarwal & Prasad, 2007) where it was found that gains in productivity is directly related to user acceptance.

Feedback and messages in connection to password creation has shown to be an important factor. However, studies have deducted different results and different approaches to implementing this. Anderson & Agarwal (2010) stress the importance of having interactive feedback, in pushing users to improve their passwords on their own terms, rather than enforce complex password policies. Hashim et al. (2010) had a different approach in their study.

Instead they created somewhat harsh feedback to users in their password creation. Such as giving warnings in red text. If the password had low security, they would also present data about how long it would take for a malicious attack to crack their password. These two studies could both benefit from the study made by Liang et al. (2019), in which they focus on user's emotion-focused-coping. In this study it is suggested that users will trigger a certain behaviour depending on the existing situation. Seeing a message saying that your password would take 10 seconds to crack, could trigger either an outwards, or inwards emotion-focused-coping. Which in theory has the potential to either improve or decrease the security of the password.

The fact that well over 60% of respondents declared a high frequency of re-usability with their passwords demonstrates similarities to previous research in the matter. Gaw & Felten (2006) found out that people tend to use somewhere between two to three passwords and alter between these amongst different applications. While the studies differ in method and hence why it could be hard to show a direct connection between the results, it still shows that some attention could be shed on the issue. Even though it has been 14 years since Gaw & Felten (2006) made their study, this provides some statistics that this issue is still present. Even with the addition of new technologies such as password managers, we have not been able to eliminate this phenom, yet.

Furthermore, the fact that a vast majority use some sort of PM, while still reusing passwords is quite alarming. The utilization of a PM fundamentally allows for an easier time managing passwords by not putting emphasis on the human mind to remember them directly. Meaning that this makes the process of adopting multiple passwords much easier. However, the survey concluded that people still tend to re-use passwords even though they use a PM. This ultimately strengthens the idea that users see PMs as a means of being comfortable, rather than utilizing it for its increased security. Suggesting that one of the big challenges for PMs is to decrease the extent to which passwords are reused.

Rogers (1995) claims that DOI reflects upon how a new idea gains momentum over time. This could be put in contrast to the different questions contained in the survey regarding usability, i.e. Q3-Q9. In other words, how each of these questions have gained momentum in the hands of home computer users. Out of all the questions in the survey, only the idea of including numbers in the password seems to have gained enough momentum to be considered at the state of laggards in the model of DOI, as can be seen in Q6 (involvement of numbers in password). Only one out of 120 respondents did not contain numbers in their password, suggesting that the idea of including numbers in the password is accepted and integrated by most users. This is also according to Rogers (1995) definition of the DOI model, proposing that this idea of innovative technological diffusion is at the final laggard state. While looking at Q7 and Q8 (involvement of upper-, lowercasing and special symbols) the result is quite the opposite of the previous question. While this way of managing passwords surely has gained momentum to some extent, there is still a long way to go until it has reached the same acceptance level as the idea of including numbers in passwords. Venkatesh et al. (2003) talk about effort expectancy and performance expectancy in their UTAUT model, something that can be used to understand why certain things are accepted from users. Looking at the sheer amount of home computer users using Google Chrome's PMs, seemingly people value what it provides. The performance expectancy of the user increases since each consecutive login becomes a shorter procedure. While this is the case, home computer users seem very content with what is being thrown in front of them, something that can be linked to effort expectancy. Google Chrome's PMs requires very little effort from the user in terms of research and

understanding, making it very accessible and easy to use. Which furthermore highlights the challenges third party PMs face. It is not enough to supply a better one in terms of security, since clearly that is not the selling point. However, it is hard to imagine that a worse product would be able to overtake a built-in system like the one that Google Chrome is offering. Hinting that PMs got to have something unique going for them, while being very easily accessible and easy to use.

The survey included mainly young individuals in the age group of 18-25 as can be found in Appendix B, Figure 6. As was concluded in Fatokun et al.'s (2019) research, the cyber security behaviours of students vary depending on age for factors like perceived severity and perceived vulnerability. It was also found that the difference in computer skills between the age groups of below and above 30 was not big enough to be presented when analysing their data findings. Given this and the limits of this study in terms of young individuals, Fatokun et al.'s research suggests that the behaviours of young individuals such as used in this research could be applicable to older individuals as well. In a study made by Carroll et al. (2001) the relationship between young individuals of similar age and technology appropriation was investigated. The research concluded that the reasons for young people's use of technology include a sense of belonging, power and to achieve a sense of cohesion by dealing with the fragmentation of their lives. Given the ease of use reason for choice of PM, it can be derived that password management differs from other technology regarding young individuals' use of technology.

Looking at Figure 13 it is apparent that around 65% of people sometimes integrate passwords they use in their private lives into their professional lives or vice versa. When put in contrast to Figure 17, it becomes evident that not a lot of respondents get motivated by their workplace to adopt the usage of PMs. This could be alarming statistics for employers, seeing as a security breach for a home computer user in many cases could be harmful to the employer, due to the sole password recycling process which is further supported by Gaw & Felten (2006). The big question is what employers can do in terms of motivating their employees to increase the overall security when it comes to password management and PMs. As suggested by Anderson & Agarwal (2010) it is preferable to allow users to feel like they command change as it promotes their own self-gratification. I.e. by giving constructive feedback on what can be improved upon etc. Employers could therefore be promoting how security breaches often are related to passwords, due to them being one of the key methods for authentication (Bachmann, 2014). By doing so, encouraging their employees to value their security. Not only would this benefit the business, but also the individual.

5.1 Implications of Practice

This study allows for a different approach to studying usability regarding PMs. Allowing us to see things through a technological perspective, such as diffusion of technology, also. This creates in-depth knowledge in the usability-security trade off. The study tells us how usability and diffusion of technology interacts with each other, that is how technological security advances such as fingerprint scanners and two steps authentication can play a role in the trade off with usability. The trade-off phenomenon is relatively well known, as it is investigated by previous research (Tam et al., 2010). However, looking into this through a more specific scope such as diffusion of technology creates more accurate data in the field of PMs.

6 Conclusion

Given the nature of IT, there is a constant development of systems that aim to be as satisfactory as possible in terms of usability and efficiency. The goal of such systems is to be both easily managed and effective in terms of its purpose. This study has investigated the effect of usability coupled with diffusion of technology on home computer users of password managers, a field that is recent and still in development. Due to it being a recent technology, the approach of this study is appropriate. As it was found in the study, ease of use was found to be the main reason behind the choice of PM, triumphing options including latest technology such as face recognition and two-factor authentication. This founding was strengthened by individuals choosing Google Chrome as the main choice of PM, which emphasizes on ease of use. Furthermore, it was found that in the trade-off between usability and security, usability was highlighted as the main priority of the two.

The result showed that the majority (65%) of people sometimes integrate passwords from private life into professional life or vice versa. However, it is also evident that not many workplaces motivate their workers to adopt the usage of PM. This allows the individual to integrate personal passwords into the workplace whose focus is on ease of use, creating a potential weakness in the workplace security. This is a direct effect on usability of home computers users in terms of PMs.

This poses a great challenge in terms of direction heading forward for PMs. While third party software might offer the best options in terms of security and diffusion of technology, this seemingly won't be the factor making them stand out from competitors. Hinting towards a shift of focus heading forward. For a PM such as LastPass to gain more recognition among users and challenge built in systems such as Chrome and Safari, they need to figure out how to be competitive in terms of ease of use and accessibility. In other words, make their system easy with little effort to master.

6.1 Future work

Seeing how the role of traditional passwords progressively is becoming more outdated, it poses the question how authorization and security will be managed in the future (Bachmann, 2014). This research has brought up how password management has been automated in the form of PMs, however there are other technologies out there who have gained momentum in the last couple of years. A good example of this is BankID, proposing a solution that is of higher user identification level and easier to handle than the traditional password. As was found in this research, ease of use is key when using digital authorization in the form of passwords. By choosing the password manager that requires the least amount of effort, people preferred ease of use over better security. By introducing an idea that focuses on ease of use but also includes high level of security, it points towards a successful user acceptance process. As has been observed lately in terms of BankID acceptance in society, it is used on a daily basis by many people (Eaton et al., 2014). Furthermore, the area of application for BankID has increased (Göransson & Asklund, 2020), showing the potential of the idea as well as the diffusion of the technology.

As was earlier found in the discussion, password management differs from other technology regarding young people's use of technology. Further investigating this idea in a more fundamental manner could further contribute to understanding why ease of use triumphs security protection with reference to young people. It could also shine light on similar issues such as the ones discussed in this research, investigating age or gender based on usability's role in password management would allow more in-depth analysis and potentially a better conclusion.

7 Appendix

Here the material for data collection will be found. Consisting of survey questions along with the data collected through these questions. This will be presented in different tables and diagrams.

Appendix A

1. What gender are you?
    1. Male
    2. Female
    3. Other (please specify)
2. How old are you?
    1. < 18
    2. 18-25
    3. 26-35
    4. 36-45
    5. 46-55
    6. > 56
3. How many characters do you tend to use in your password?
    1. < 9
    2. > 9
4. Are you using different passwords for different applications?
    1. Always a different password for each application
    2. Often a different password for each application
    3. Same password often occurs
5. Do you often switch your passwords not to match any older version that you've used?
    1. Never
    2. Sometimes
    3. Often
    4. Always
6. Does your password contain numbers?
    1. Yes

2. No

7. Does your password contain special symbols? (!, @, % etc.)

1. Never
2. Sometimes
3. Often
4. Always

8. Does your password involve both upper- and lower casing?

1. Never
2. Sometimes
3. Often
4. Always

9. Do you often use the same passwords for your professional- and personal life?

1. never
2. sometimes
3. often
4. Always

10. Do you use a password management system to help you manage your passwords?

If yes, which one:

1. Google Chrome (built in)
2. Dashlane
3. LastPass
4. 1Password
5. RoboForm
6. Other (Optional for textbox)

11. What makes it intriguing to you to use a certain type of password manager that is different from the rest?

1. Latest technologies such as fingerprints

2. Face recognition
3. Two-factor authentication
4. Ease of use/flexibility
5. Other (Optional for textbox)

12. What password management system do you focus on when it comes to helping you manage your passwords?

1. Google Chrome (built in)
2. Dashlane
3. LastPass
4. 1Password
5. RoboForm
6. Other (Optional for textbox)

13. If you use any password management system, what makes it stand out from the rest of systems that are available to you?

1. Latest technology in authentication
2. Ease of use
3. Popularity
4. Influenced by the workplace
5. Other (Optional for textbox)

14. Are you familiar or use any of the following password management systems?

1. Roboform
2. Dashlane
3. rememBear
4. Kaspersky
5. NordPass
6. LastPass
7. 1Password

8. Sticky xxx
9. KeePass Password Safe
10. Keeper Password Manager
11. Enpass
12. Zoho Vault
13. Bitwarden
14. Other (Optional for textbox)

15. As a last remark on passwords and password management systems for home computer users, do you have any specific recommendations that are worth pointing out?

1. Optional textbox

Appendix B

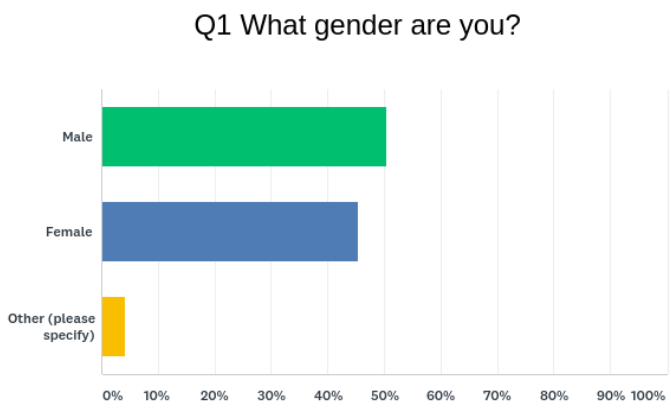

Figure 5

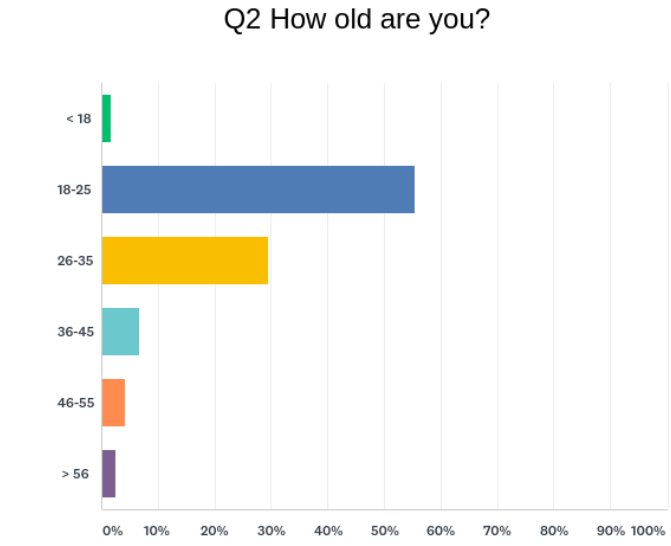

Figure 6

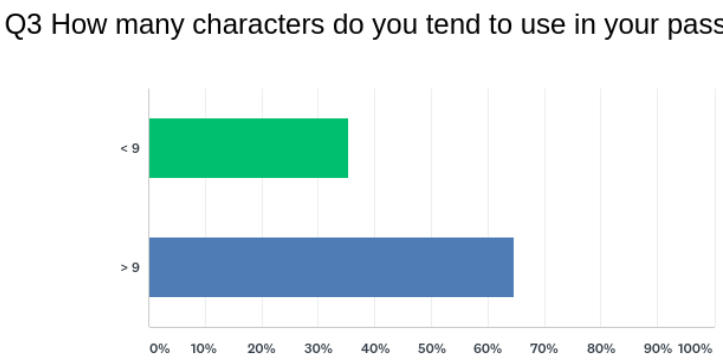

Figure 7

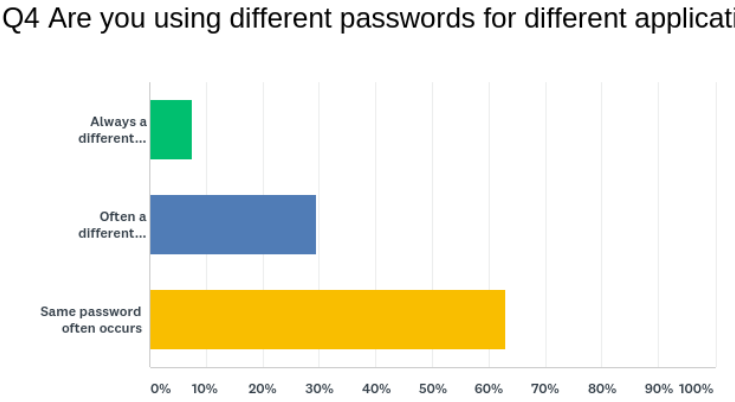

Figure 8

Q5 Do you often switch your passwords not to match older version that you've used?

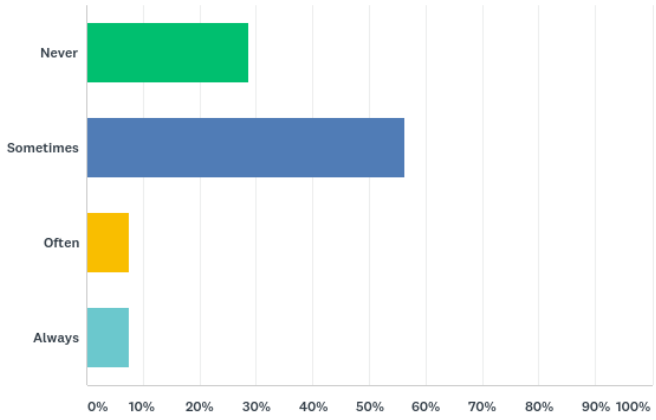

Figure 9

Q6 Does your password contain numbers?

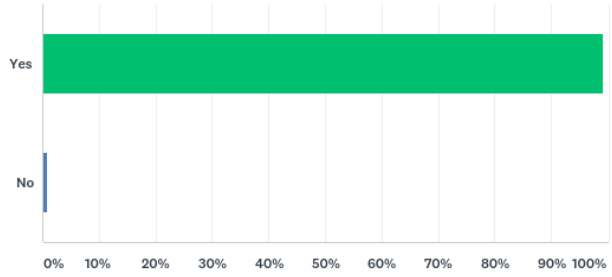

Figure 10

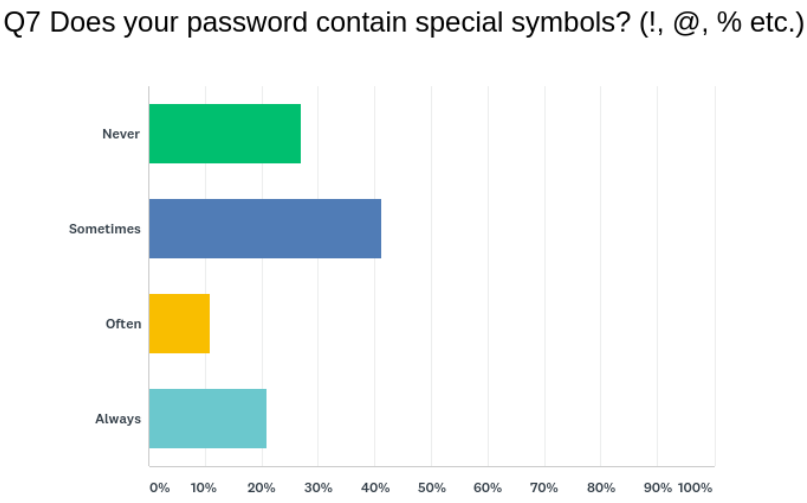

Figure 11

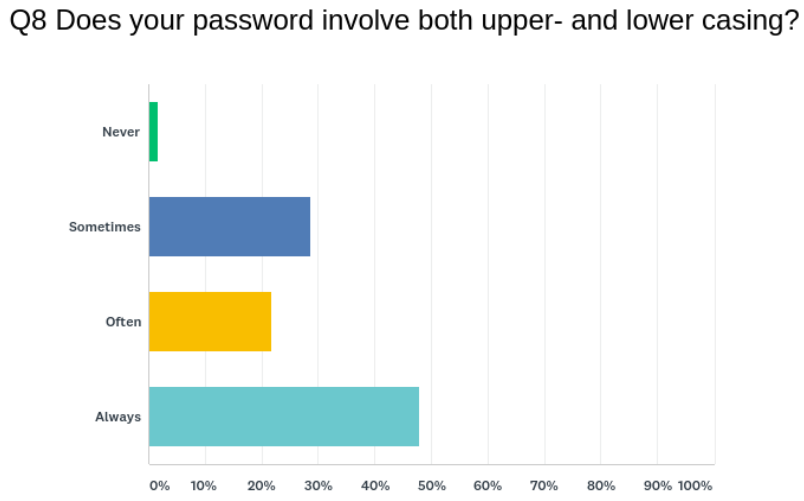

Figure 12

Q9 Do you often use the same passwords for your professional- and personal life?

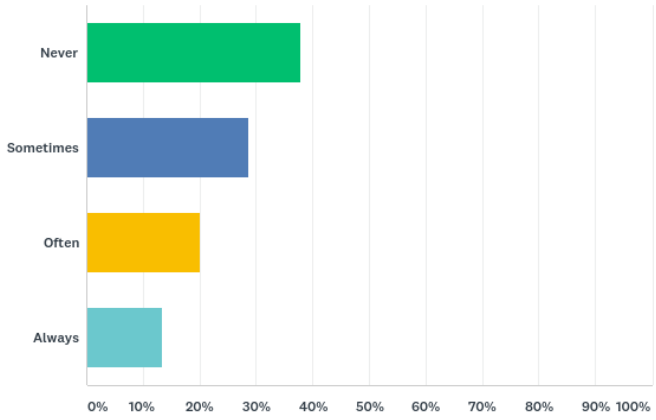

Figure 13

Q10 Do you use a password management system to help you manage your passwords? If yes, which ones:

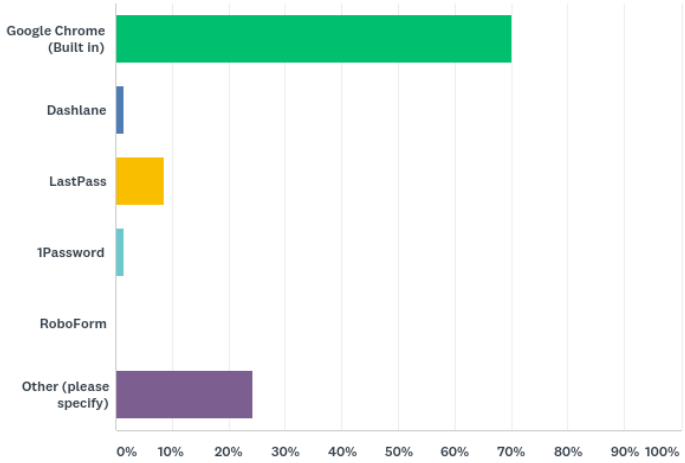

Figure 14

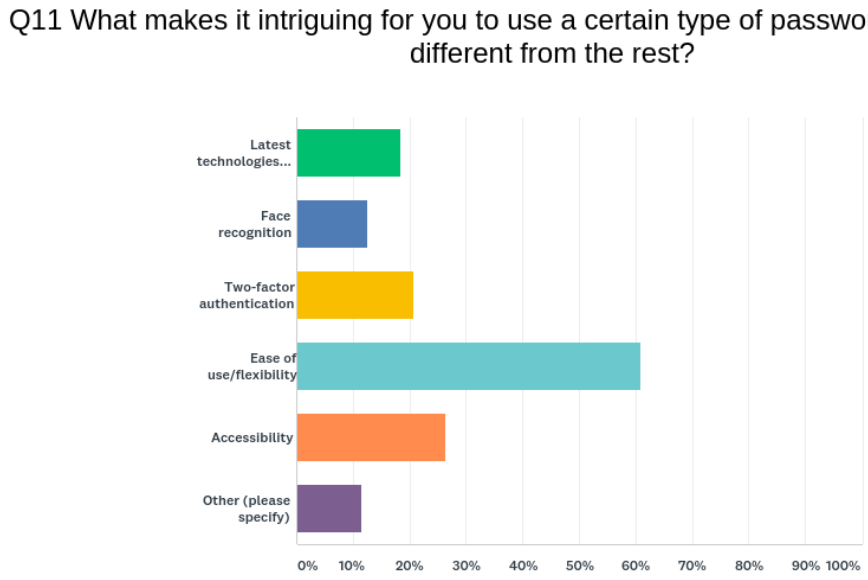

Figure 15

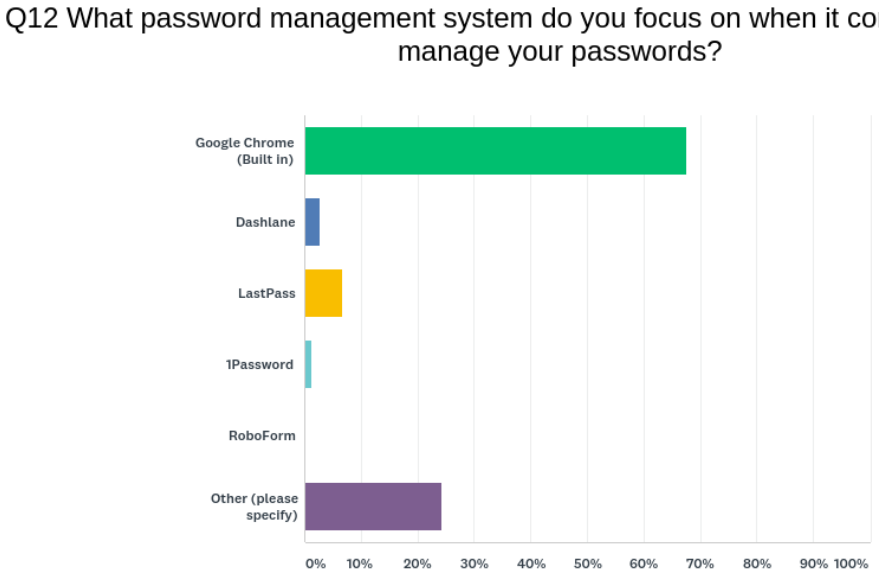

Figure 16

Q13 If you use any password management system, what makes it stand out from the rest of systems that are available to you?

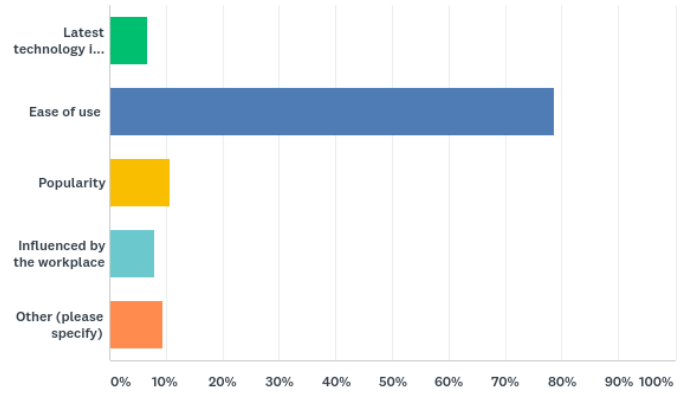

Figure 17

Q14 Are you familiar or use any of the following password management systems?

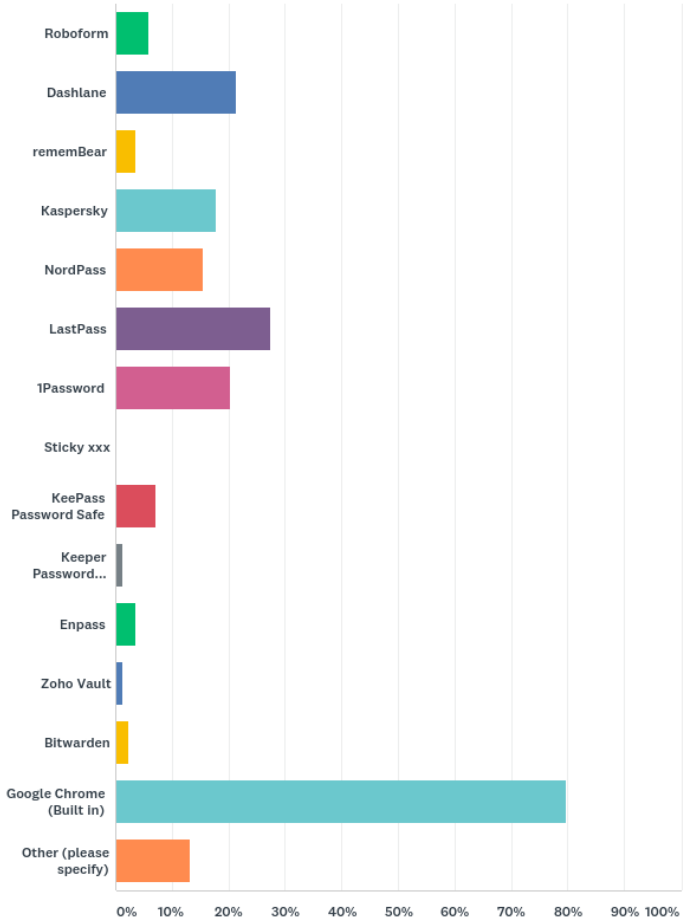

Figure 18

8 References

Agarwal, R. & Prasad, J. (2007) *The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies*.

Anderson, C. L. and R. Agarwal (2010) *Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions*, in International Conference on Information Systems, pp. 1543-1561. Milwaukee, WI.

Bachmann, M. (2014, September). *Passwords are Dead: Alternative Authentication Methods*. In 2014 IEEE Joint Intelligence and Security Informatics Conference (pp. 322-322). IEEE.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010) *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness*. MIS Quarterly, 34, 3, 523-548.

Carrol, J., Howard, S., Vetere, F,. Peck, J. & Murphy, J. (2001) *Identity, Power And Fragmentation in Cyberspace: Technology Appropriation by Young People.* ACIS, 6.

Cazier, J. & Medlin, B. (2006) *How secure is your password? An analysis of E-commerce passwords and their crack time.*

Chen, Y. & Zahedi F. (2016) *Individuals' Internet Security Perceptions and Behaviors: Policontextual Contrasts Between the United States and China*. MIS Quarterly, Vol. 40, No. 1, pp 205-222.

Cimpanu, C. (2018). State Department shamed for poor adoption of multi-factor authentication. [url:https://www.zdnet.com/article/state-department-shamed-for-poor-adoption-of-multi-factorauthentication].

Dayem, L. (2018) The Ethics of Cyber Warfare. University of Chicago. Vol. 4, No. 1.

Eaton, B., Hallingby, K. H., Nesse, P. & Hanseth O. (2014). *Achieving payoff from an industry Cloud Ecosystem at BankID.* MIS Quarterly Executive, 13, 4. 229.

Fatokun, F., Fatokun, J., Hamid, S. & Norman, A. (2019) *The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviour of Tertiary Institution Students: An Empirical Investigation on Malaysian Universities.* Journal of Physics: Conference Series, Volume 1339, International Conference Computer Science and Engineering (IC2SE) 26-27 April 2019, Padang, Indonesia.

Gaw, S. & Felten E. W. (2006) *Password Management Strategies for Online Accounts*

Göransson, A. & Asklund, E. (2020) *BankID-based Authentication for Phone Calls*. LU, LTH-EIT 2020-741.

Hashim, M., Khern-am-nuai, W., Li, N., Pinsonneault, A & Yang, W. (2010). *Practicing safe computing: a multimedia empirical examination of home computer security.*

Liang, H., Xue, Y,. Pinsonneault, A. & Wu, Y. (2019) What users do besides problem-focused coping when facing security threats: An emotion-focused coping perspective. MIS Quarterly, Vol. 43, No. 43.

Mackie, I., Yildirim, M. (2019) Encouraging users to improve password security and memorability. International Journal of Information Security 18, 74-759.

Malgas, G., O'Brien, J. A. (2006) Introduction to information systems. McGraw-Hill, Inc. Professional Book Group 11 West 19th Street New York, NY, United States
ISBN: 978-0--07-304355-5

Mata, F., Fuerst, W. & Barney, J.(1995) *Information Technology and Sustained Competitive Advantage: A Resource-Based Analysis*. MIS Quarterly, 19, 4, 487-505.

Moody, G. D., Siponen, M. & Pahnila, S. (2018) *Toward a Unified Model of Information Security Policy Compliance.* MIS Quarterly. 42. 285-311.

Moore, D., Paxson, V,. Savage, S,. Shannon, C,. Staniford, S. & Weaver, N. (2003) *The Spread of the Sapphire/Slammer Worm*, Tech. rep., CAIDA, ICSI, Silicon Defense, UC Berkeley EECS & UC San Diego CSE.

Osborne, C. (2019) *These are the worst hacks, cyberattacks, and data breaches of 2019*. ZDNet.

Porter, M. (1990) *Competitive Advantage of Nations: Creating and Sustaining Superior Performance*, United States of America, Free Press.

Preece, J., Rogers, Y,. Sharp, h., Benyon, D,. Holland, S & Carey T. (1994) Human-Computer Interaction. Addison-Wesley Longman Ltd, Edinburgh Gate Harlow, United Kingdom.

Rogers, E. M. (1995) Diffusion of Innovations. 4th ed. New York, Free Press.

Venkatesh, V., Morris, M., David, G. & Davis, F. (2003) User Acceptance of Information Technology: Toward a Unified view. MIS Quarterly, 2003, 27,3, 425-478.

von Solms, R & van Nierkerk, J. (2013) From information security to cyber security. School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth 6031, South Africa.

Statista (2020). *Digital Population Worldwide.*
Retrieved 5/4-20 https://www.statista.com/statistics/617136/digital-population-worldwide/

Tam, L., Glassman, M. & Vandenwauver, M. (2010) The psychology of password management: a tradeoff between security and convenience, Behaviour & Information Technology, 29:3, 233-244, DOI: 10.1080/01449290903121386.

Techopedia (2020) *Password Manager*.
Retrieved 10/4-20: https://www.techopedia.com/definition/31435/password-manager

Turban, E. (2008) *Information Technology for Management*. John Wiley & Sons, Inc., USA. 5th ed.

Wei, W. (2017) *The Hacker News; 9 Popular Password Manager Apps Found Leaking Your Secrets*
Retrieved 15/5-20: *https://thehackernews.com/2017/02/password-manager-apps.html*