Aleksi Myntti

PASSWORD MANAGERS: A CAUSE OR AN ALLEVIATOR OF TECHNOSTRESS?

UNIVERSITY OF JYVÄSKYLÄ
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

ABSTRACT

Myntti, Aleksi
Password Managers: A Cause or an Alleviator of Technostress?
Jyväskylä: University of Jyväskylä, 2023
Information Systems Science
Supervisor: Woods, Naomi

Password managers helps their users to create, manage and store secure password. Even though they are widely considered a good option to manage passwords, they are often underutilized tools to improve password security. Although previous research has extensively studied password manager usage and security, no studies have been conducted to examine password managers in relation to technostress. A quantitative survey was conducted to measure technostress experienced by password manager users and non-users. Additionally, survey respondents were presented an optional open question to ask why they choose to use or not use password managers. The survey results revealed that users of password managers experience significantly less technostress compared to non-users. Furthermore, from the open question, it was revealed that users primarily use password managers for the password memorability, improved password security, convenience, and easier password management. Non-users reported their lack of use primarily due to distrust, a lack of necessity, inactivity, and reluctance. These findings provide opportunities for a better understanding of password management software and its potential causes for technostress which can result in improved password managers and increased password security.

Keywords: password managers, technostress, passwords, internet

TIIVISTELMÄ

Myntti, Aleksi
Salasananhallintaohjelmistot: Teknostressin aiheuttaja vai lieventäjä?
Jyväskylä: Jyväskylän yliopisto, 2023
Tietojärjestelmätiede
Ohjaaja: Woods, Naomi

Salasananhallintaohjelmistot auttavat käyttäjiään luomaan, hallinnoimaan ja varastoimaan turvallisia salasanoja. Vaikka niitä yleisesti pidetään hyvänä vaihtoehtona salasanojen hallinnointiin, ne ovat edelleen laajalti vähän käytettyjä työkaluja salasanaturvallisuuden parantamiseen. Vaikka aikaisemmat tutkimukset ovatkin tutkineet laajasti salasananhallintaohjelmistojen käyttöä ja turvallisuutta, ei ole suoritettu tutkimuksia, jotka tarkastelisivat salasananhallintaohjelmistojensuhdetta teknostressiin. Salasananhallintaohjelmistojen käyttäjien ja ei-käyttäjien kokemaa teknostressiä mitattiin määrällisellä kyselytutkimuksella. Lisäksi kyselyyn osallistuneilta kysyttiin vapaaehtoisella avoimella kysymyksellä miksi he käyttävät tai eivät käytä salasananhallintaohjelmistoa. Kyselyn tuloksista saatiin selville, että salasananhallintaohjelmistojen käyttäjät kokevat ohjelmistosta selvästi vähemmän teknostressiä kuin ei-käyttäjät. Lisäksi avoimesta kysymyksestä selvisi, että käyttäjät käyttävät salasananhallintaohjelmistoja pääasiassa salasanojen muistettavuuden, tietoturvan, kätevyyden ja helpomman salasananhallinnan takia. Ei-käyttäjät kertoivat käyttämättömyytensä johtuvan pääasiassa epäluottamuksesta, tarpeen puutteesta, epäaktiivisuudesta ja vastahakoisuudesta. Tulokset avaavat mahdollisuuksia parempaan ymmärrykseen salasanahallintaohjelmistoista ja niiden mahdollisesti aiheuttamasta teknostressistä, jonka ansiosta voidaan kehittää parempia salasananhallintaohjelmistoja ja parantaa salasanaturvallisuutta.

Avainsanat: salasananhallintaohjelmisto, teknostressi, salasanat, internet

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Need for secure password and good personal security is increasingly important as number of online services has skyrocketed in the past years. In corporate IT environment there is a massive number of employees that systematically repeat that there is an overwhelming number of services that require a log-in with a strong enterprise password policy (Arias-Cabarcos, Marín, Palacios, Almenárez & Díaz-Sánchez, 2016). It is widely known that a good password is not as easy to remember as a bad password and many of the flaws in modern password authentication systems comes from human memory limitations (Yan, Blackwell, Anderson & Grant, 2004). If a user is forced to create a good password, they will write it down somewhere visible such as on a post-it note (Gaw & Felten, 2006). While poor password usage might not be very damaging for an individual user, it can be massively damaging for included company (Arias-Cabarcos et al. 2016). Password manager is an often proposed but still not very widely used solution (Fagan, Albayram, Khan & Buck, 2017). This is regardless that studies show that security experts frequently recommend using Password Managers (Ion, Reeder & Cosolvo, 2015). This master's thesis explores reasons behind scarce usage of password managers and whether technostress can be a factor behind this.

1.1 Motivation and research problem

This thesis explores whether disuse of password managers is related to technostress. The thesis examines password managers in general and does not focus in one specific password manager type, e.g., desktop application or browser integrated password manager. It is very important to understand technostress as the help of ICTs can aid users in repetitive tasks and allows them to create new working techniques, use time more efficiently and improve their technological skills, but these benefits can coexist with feelings of frustration and distress (Brod, 1984, Hudiburg, 1989, as cited in Ragu-Nathan, Tarafdar & Ragu-Nathan, 2008). There are existing studies that explores password manager usage and

technostress formation but there are currently no studies that measures technostress that is caused by password managers. This study aims to fill some of that research gap by measuring technostress between two groups, password manager users and non-users, and whether there is a difference in technostress levels between those two groups. Ultimately, understanding whether password managers can cause technostress may potentially lead to better password managers which can cause fewer people to be less reluctant towards them.

Technostress and password managers are widely studied fields with new studies coming out frequently. The topic for this thesis was chosen because there is a massive research gap in password manager and technostress studies and there is a need for a study which directly measures and compares technostress caused by password managers in users and non-users. This thesis aims to contribute to existing technostress and password manager research by providing insight to minds of password manager users and non-users. This thesis uses model for understanding technostress proposed by Ragu-Nathan et al. (2008) which is derived from Transactional-Based Model approach for stress (Lazarus, 1966, McGrath, 1976, Lazarus & Folkman, 1984, as cited in Ragu-Nathan et al., 2008), and a study by Tarafdar, Ragu-Nathan & Ragu-Nathan (2007) to understand and measure technostress caused by password managers. This thesis aims to answer the following research questions:

1. Do password managers cause technostress?
2. Is there a difference between in technostress levels between password manager users and non-users?

The research questions will be answered by measuring technostress using a survey and analysing the results comparing the responses between password manager users and non-users. The results contribute to existing password manager and technostress research. The results have the potential to pave the way for future research on password managers and their role in technostress, enabling a more accurate identification of the underlying causes of technostress caused by these tools.

1.2 Literature review

The theoretical background for this study is mainly based on existing literature of stress and technostress with a slightly lesser focus on password manager studies. Various online sources, search engines, internet libraries and databases were utilized to conduct an extensive literature review on studies and literature of stress, technostress, and password managers. The main sources for articles and studies were search engine Google Scholar and internet libraries such as ACM Digital Library and ResearchGate. The literature review aimed to find out a research gap and what already is known about password managers and technostress. It was found that there is no existing literature that measures

technostress caused by password managers. The studies on technostress by Tarafdar et al., (2007) and Ragu-Nathan et al., (2008) are at the core of this literature review. Based on these studies, survey questions were formed, and a survey was conducted which aimed to measure technostress on four different areas of technostress, known as technostress creators, presented by Tarafdar et al., (2007). These measured technostress creators in this study are techno-overload, techno-invasion, techno-complexity, and techno-uncertainty.

The literature review on password managers was conducted to shed light on their features and functionalities, as well as to understand what is already studied about their usage and users' attitudes towards them. Additionally, the literature review on password managers aimed to present research information regarding their impact on cybersecurity and their potential concerns. It was found that while core principles and functionalities are mostly the same, password managers differ significantly in their qualities and functionalities, as they have varying database formats, platform compatibility, cloud storage accessibility, and the availability of their source code (Gasti & Rasmussen, 2012). The literature review also found that password managers are mainly used to ease the burden of remembering passwords and increased security, while non-users reported that main reasons to not use a password manager are security concerns, lack of need, lack of motivation and usability concerns (Fagan et al., 2017).

1.3 Thesis outline

The second chapter discusses password managers in general and explores their core principles and functionalities. This chapter explores how and why password managers are used, how they work, and what kind of advantages or disadvantages it has on personal or organizational cybersecurity. Password manager weaknesses and concerns are also explored in this chapter.

The third chapter, which is the other chapter of literature review, discusses existing technostress studies and what is already known about it. The brief history and background of stress and technostress studies are discussed, along with the current understanding of how technostress forms in individuals. The subdomains of technostress are also discussed and what factors influence the formation of technostress. The thesis hypotheses are then formed based on existing studies on technostress and password management software.

Finally, empirical chapters of this thesis present the used research methods and more accurately describes the research process and procedures. The results of the survey analyses are then presented, and hypotheses are answered. Further on, contributions and practical implications are reflected on and limitations and possibilities for future research are considered. The final chapter concludes the thesis with a conclusion of the findings.

2 PASSWORD MANAGERS

A Password Manager is a software that helps users to store, create and organize passwords. Password managers have all the same general functionality principles. Fundamentally, a password manager acts as a database for user's usernames and passwords for different sites and services and they are secured with a master password (Li, Hem Akhawe & Song, 2014). Application creates a local database to store saved passwords and encrypts them to ensure their safety and protection. (Arias-Cabarcos et al. 2016). This leaves user with only one memorisable password, the Master Key which gives access to all stored passwords. Depending on the password manager, the passwords can be stored to either a cloud service or locally. Password managers are often presented as a user-friendly way to store your passwords to different services. There are few new authentication technologies emerging to improve security, such as Single Sign-On (SSO) protocols, but passwords remain the dominant method of authentications and PMs offer users an alternative for immediate usage without any preparations or infrastructure modifications (Arias-Cabarcos et al. 2016). Different Password Managers have varying qualities and functionalities. Password managers may have differences in database format, platform support and cloud storage access and source code availability. (Gasti & Rasmussen, 2012.)

At their core, passwords managers operate in a very similar way. Figure 1 illustrates how a password manager is used to login to a web application. **Step 1**: Using master username and password, a user logs into the password manager. **Step 2**, the user receives his or her credentials for the chosen web application from the password manager. **Step 3**, the user uses credentials to login to the web application. **Step 4**, the user gains access to the web application.

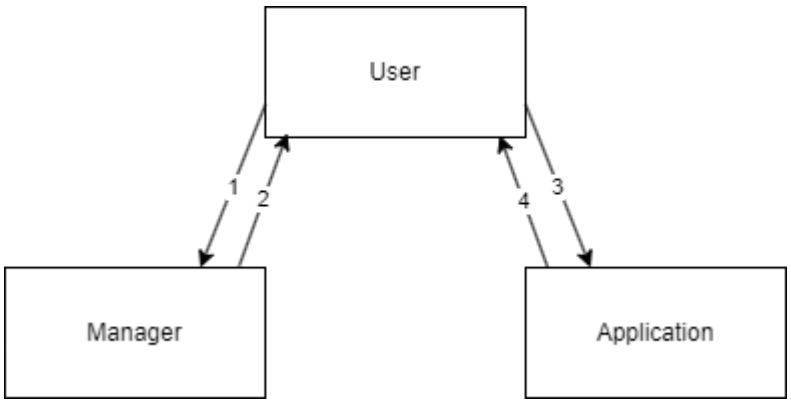

Figure 1. Different parties in a password manager scheme (Li, He, Akhawe & Song, 2014)

2.1 Password manager usage

Because of password managers' well-known benefits of alleviating burden of remembering passwords and increasing security, many popular media publications and security experts recommend using password managers (Li et al., 2014). According to previous studies, users often adopt usage of browser-based password managers without forethought because users tend to click through browser's popups and start using browser manager even if they are already using an external password manager (Oesch, Ruoti, Simmons & Gautam, 2022). Built-in password managers, such as browser-integrated or password mangers integrated into operating system, are mainly used for convenience and separate password manager tools are more frequently used for security reasons (Pearman et al., 2019) Previous studies suggests that built-in password managers, such as browser-integrated or password mangers integrated into operating system, are mainly used for convenience and separate password manager tools are more frequently used for security reasons (Pearman et al., 2019). Mobile password managers are generally less frequently used, as mobile interface usually doesn't have a consistent autofill and password autosave functionalities (Oesch et al., 2022).

Password manager users report that main reasons to use a password manager are to make remembering a number of complicated passwords easier and to increase password security while non-users report that reasons to not use a password manager are security concerns, lack of need, lack of motivation and usability concerns (Fagan et al., 2017). Adoption of password managers most often come from users' need to use a password manager at work, to make logins to different services easier or to improve their password quality. Online security typically comes second on users' priority list when it comes to using services (Whitten & Tygar, 1999). Users view password manager usability in a very positive way (Silver, Jana, Boneh, Chen & Jackson, 2014). A previous study showed that encouraging user autonomy, relatedness and competence improves user adoption for password managers (Alkaldi, Renaud & Mackenzie, 2019). Autonomy in this context means that using non-demanding language and giving user

options increases adoption rate. Relatedness means offering some kind of connectivity to target behaviour. Competence means that offering clarity, positive feedback and guidance can ease the adoption of the password manager.

2.2 Password manager security

While the core principles between different password managers remain the same, there are certain differences between different password managers and their functionalities can have a drastic effect on the password security. Password manager security can be studied in three major categories: *Security of the Master Key, Security of the Credentials* and *Security of Communications* (Arias-Cabarcos et al., 2016).

Security of the Master Key is one of the most crucial parts of successfully utilizing a password manager, as the Master Key is essential for the safe usage of a password manager. Some password managers are better at keeping the Master Key safe than others. More secure password managers may have a minimum length requirement for the Master Key and force the user to comply with a secure policy to create a strong password. Lastly, password managers differ in the way how they store the Master Key. (Arias-Cabarcos et al., 2016).

Security of the Credentials database is almost equally important since the credentials database is like the vault of gold for password manager it is important that they are well encrypted. Some password managers have better encryptions than others or may have other authentication options to access credential database such as multifactor authentication (Arias-Cabarcos et al., 2016). Encrypting the credential database locally on the user's computer is one of the more common methods to secure the passwords, preventing passive attackers from accessing the passwords in text form. The password manager is able to encrypt and decrypt passwords on the user's side using a decryption key, which can be derived from user's master key credentials. (Li et al., 2014). Security of Communications. Password managers can communicate credentials between external cloud servers or browser applications, and they differ in ways in how they secure their communications.

A study by Luevanos et al. (2017) has explored differences in security on open-source and closed source password managers. Open-source itself seems to be the greatest strength of this type of password managers, as the open code enables users to freely examine the code and identify possible security weaknesses to its developers, but on the downside, this leaves the password manager more vulnerable to bugs and security weaknesses as they are generally found at a slower pace. Another problem with open-source password managers is that not every user report security problem and this can open opportunities for the attackers in the future. On the other hand, closed source password managers have some benefits over closed source password managers, as closed source keeps

their code hidden from potential attackers. This makes certain types of attacks, such as fake extensions, are less effective. The most central problem with a closed source password manager is the company behind it. This means, that user has to trust the company behind the password manger to keep their passwords safe and provide constant updates to keep their passwords secure and it also means fewer eyes looking at the code and finding weaknesses. (Luevanos et al., 2017.)

Newer and more modern password managers often provide its user more convenient way to authenticate and secure their password usage. Newer password managers have features such as collaboration. Collaboration feature has the ability to share encrypted credentials at the request of the credential owner. When requested, the password manager shares the credentials with other password manager user without giving the person who the credentials are shared with an access to the password itself. (Li et al., 2014). Password manager autofill functionalities also serve a part in password manager security. Password managers varies in their autofill policies and can put their users at risk depending on domain. A previous study found that several commonly used password managers are vulnerable to autofill-based password extraction attacks when using a malicious free WiFi hotspot. (Silver, Jana, Boneh, Chen & Jackson, 2014).

2.3 Password manager benefits

Passwords are the most widely used yet rather unsecure form of authentication (Chiasson, Oorschot & Biddle, 2006). Password managers has been created to alleviate a common problem among internet users and workers: the number of complicated passwords that individuals are required to remember is easily exceeding human limitations and creates nearly impossible barriers for secure and safe password practices. When users have a large number of passwords to remember, they often fall into bad password practices (Arias-Cabarcos et al., 2016). There are practical methods to help the burden of having a massive number of passwords. For example, using passphrases can help users to create stronger passwords but it does not help users to manage multiple passwords across multiple accounts (Chiasson, Oorschot & Biddle, 2006).

Bad password practices are harmful for individual users, but the damage is worse for companies as an employee could leak sensitive data to an attacker and potentially cause business or reputation damage (Arias-Cabarcos et al., 2016). Even though various log-in systems and password policy guidelines use and recommend restrictions to passwords, such as minimum number of characters, prohibited reuse and impose frequent modifications to your passwords, previous studies have shown that instead of increasing security, hard restrictions drive users to bad password practices. (Inglesant & Sasse, 2010). Previous study has also found that differing password policies that do not match with users' leads to users not being motivated to use secure practices (Inglesant & Sasse, 2010).

Using a password manager can offer its users relief to the burden of remembering all of their passwords to different services. Instead of using mnemonics or

similar tools to alleviate the problem, a password manager can be a helpful tool for individuals. Interestingly, even though security experts frequently recommend using a password manager, they are still not very widely used (Fagan et al., 2017). Password managers offer a variety of tools to help their users not only to manage and create safe passwords, but to use them safely as well. Password managers offer stronger protection against phishing websites and typo-squatting as the PM stores full URL alongside their password offering, which means that PM won't fill the password when visiting a malicious website (Gasti & Rasmussen, 2012; Li et al., 2014). Password managers can also notify users about passwords that are either compromised or weak. Password managers can also notify its users about passwords that are either compromised or weak. (Oesch, Ruoti, Simmons & Gautam, 2022). It has been found that convenience is a major factor when considering password manager usage, as previous study has shown that people who use password managers considers their usefulness and convenience as the main reasons for using a password manager. Users and non-users of password managers often misunderstand the purpose of a password manager as they tend to use a password manager for convenience and non-users chooses to not use a password manager because of security concerns. (Fagan et al., 2017).

2.4 Password manager weaknesses and security concerns

Password managers are generally believed to increase security (Luevanos, Elizarraras, Hirschi & Yeh, 2017). However, password managers are found to have a variety of different kind of weaknesses and security concerns. Causes of these concerns varies from poorly utilized usage and software related problems.

Previous studies have revealed that users may not take advantage of password managers' features and they may have unexpected ways of compromising their password security. For example, users may completely ignore the manager's random password generator and choose to use reused and weak passwords (Oesch, Ruoti, Simmons & Gautam, 2022; Pearman, Zhang, Bauer, Christin & Cranor, 2019). Oesch et al. (2022) found that this is due to users' fear that they would need to use their passwords on devices that do not have their password managers installed. Other studies have identified several security concerns on web-based password managers. Li et al. (2014) found diverse field of problems ranging from authorization mistakes and logic to web security model misunderstandings. A study by Fagan et al. (2017) suggests that people that do not use password managers may not fully understand how they work and even users may not have a full understanding of security benefits that a password manager offers. Same study also revealed that non-users note security issues as the main reason why they opted not to use a password manager. Previous study also points out an increasing need for password managers to support cross-device support (Oesch, Ruoti, Simmons & Gautam, 2022).

In summary, password managers are used for a variety of reasons, mainly to relieve the burden of remembering a large number of complicated passwords

and to increase security. People not using password managers tend to not use them because if security concerns, they do not need them, or they don't have the time or motivation to learn their use. Password manager security consists of security of the master key, security of credentials and security of communications. Password managers offer a variety of benefits, most importantly increasing security for individuals and organizations alike. Password managers also have potential security concerns which are mostly related to human error or not utilizing their features properly.

3 TECHNOSTRESS

In this chapter, technostress is introduced. Initially, the background and definition of technostress will be gone through, after which the theoretical frameworks related to the formation of technostress will be examined. Finally, the causes of technostress and how it affects individuals will be explored.

3.1 Technostress background

In colloquial language, stress refers to a negative feeling of burden or pressure. *Being under stress* is a situation where an individual experiences a perceived demand which is threatening to surpass his or her resources and capabilities for meeting the demand where the individual expects a notable differential in the rewards and costs for being able to meet the demand or not meeting it (McGrath, 1976, as cited in Ragu-Nathan et al., 2008). Stress is a common phenomenon and is known to cause a variety of problems. Stress has been found to reduce happiness, tensing relationships between people and reduce productivity of employees (Salo & Pirkkalainen, 2019). Early studies focusing on organizational use of ICT describes various end-user experiences to ICT, like anxiety (Heinssen, Glass & Knight, 1987), unhappiness with work and a higher feeling of work pressure (Smith & Salvendy, 1991, as cited in Ragu-Nathan et al., 2008).

The term technostress refers to a stress which is caused by the use of information technology (Tarafdar, Pirkkalainen, Salo & Makkonen, 2020). The term was first used by psychologist Craig Brod in the 1982 when he was observing usage of home computers by the people at home or workplaces. Brod (1984) defines the term technostress as a modern disease of adaption which is caused persons difficulty to adapt to a new technology in a healthy manner. It is suggested that technology itself can be at the core of the problem and cause of technostress instead of just being experienced by the user (Salo & Pirkkalainen, 2019). This is further supported by the fact that stress is often experienced in life-changing situations and being confronted by a new type of technology can feel overwhelming

for the new user (Salo & Pirkkalainen, 2019). Technostress is experienced when people are unable to adapt to information technology properly and it becomes a fundamental part of our daily lives forcing us to stay linked all the time (Tarafdar, Pullins & Ragu-Nathan, 2014). Users can also experience technostress if they feel they do not possess required skills to effectively use ICT and the user can feel stressed if they feel that they cannot follow constantly evolving ICT and frequently changing physical, social, and cognitive requirements in order to use ICT effectively (Tarafdar & Ragu-Nathan, 2010). Early studies focusing on organizational use of ICT describes various end-user experiences to ICT, like anxiety (Heinssen, Glass & Knight, 1987), unhappiness with work and a higher feeling of work pressure (Smith & Salvendy, 1991, as cited in Ragu-Nathan et al., 2008). As current workplaces and organizational environments are increasingly more knowledge intensive, operations are being outsourced and collaboration is more common between organizations, individuals are increasingly required to engage in ICT interactions on a daily basis (Ragu-Nathan et al., 2008). Increasing number of users seem to be searching for a way to alleviate fatigue that remembering multiple passwords causes and password manager is widely recommended as an answer (Li, He, Akhawe & Song, 2014). However, learning to use a password manager is another software for a person to learn and a potential cause for additional technostress. In addition to that, previous studies have shown intensive ICT users to experience less technostress than non-intensive users (Salanova, Llorens & Cifre, 2013). Therefore, I hypothesize that:

H1: There will be a difference in technostress between password manager users and non-users.

3.2 Technostress formation

Existing literature on technostress is heavily based on fundamental studies on stress. The Transaction-Based approach (Lazarus, 1966, McGrath, 1976, Lazarus & Folkman, 1984, as cited in Ragu-Nathan et al., 2008) is functioning as a foundation to understand how technostress is being formed. The model describes stress as a stimulation combined with individual's response. In the model, *stressors* are events or conditions that individuals encounter in a work or organizational environment, including but not limited to, increased workload, uncertain career path, and changes in colleagues (Cartwright & Cooper, 1997). Additionally, stressors can be events that has happened only once, such as traumatizing life-threatening situation or continuous problems that occur over a longer period of time (Sonnentag & Frese, 2013).

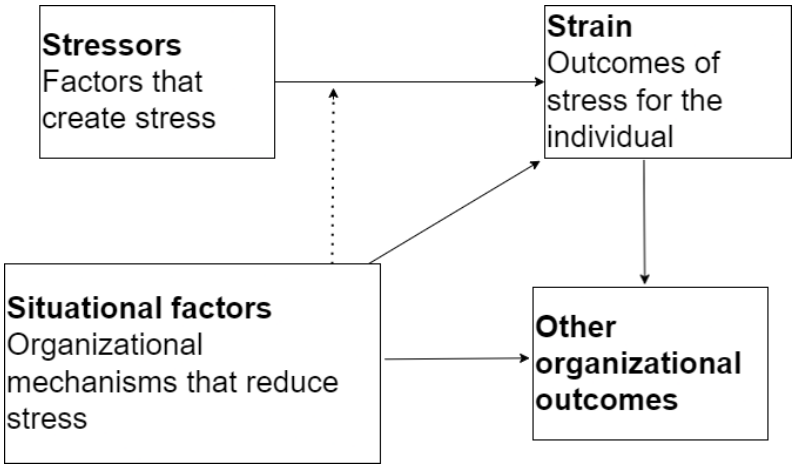

Figure 2. Transactional-Based Model of Stress (Ragu-Nathan, Tarafdar & Ragu-Nathan, 2008)

Stressors can be either role-related, or task-related. Role-related stressors are mostly related to individual's role in an organization and are related to things such as role ambiguity, role conflict, and role overload (Kahn, Wolfe, Quinn, Snoek & Rosenthal, 1981, Rizzo, House & Lirtzman, 1970, Ivancevich and Matteson, 1980, as cited in Ragu-Nathan et al., 2008). Task-related stressors on the other hand describes task properties that can potentially cause stress for the individual, such as task ambiguity or difficulty (McGrath, 1976). *Situational factors* are different kind of organizational functions or mechanisms that helps to reduce the effect of stressors, which includes factors such as role restructuring, job redesign, stress management training and social support (Burke 1993, Davis & Gibson, 1994, as cited in Ragu-Nathan et al., 2008). *Strain* refers to different kind of outcomes that is caused by the stress itself, and can be experienced by the individual as behavioral, physical, or psychological effects. Stressors and strain have a positive relationship, which means that stressors increase strain. And finally, *other organizational outcomes* are different kind of outcomes that strain can lead to. For example, long-standing employee stress can cause absences and thus negatively affect the company financially (Ragu-Nathan et al., 2008).

Based on earlier study on stress and the Transactional-Based Model of Stress, Ragu-Nathan et al. (2008) proposed a new model to understand how technostress is formed. The study suggests a conceptual model to understand how technostress is caused and what affects how an individual experiences it. The two models are similar in structure and function with a few key differences. *Technostress creators* are factors that create technostress, and it is comparable to *stressors* in Figure 2. Technostress creators will be explored further in the part 3.2. *Technostress inhibitors* are organizational functions and mechanisms that have an effect to alleviate technostress and it is parallel to *situational factors* in Figure 2. An example of a technostress inhibitor would be end-users' involvement during a new system's implementation phase as earlier study has shown it having an alleviating effect on their technostress (Brod, 1984). *Job satisfaction* in Figure 3 is

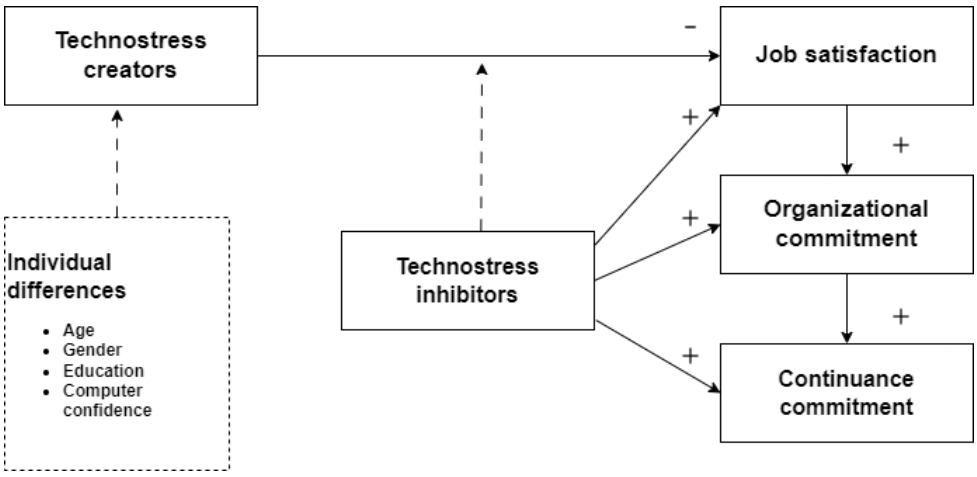

Figure 3. Conceptual Model for Understanding Technostress (Ragu-Nathan, Tarafdar & Ragu-Nathan, 2008)

inversely parallel to *strain* in Figure 2. Job satisfaction means a positive state of mind which is a result of the appraisal of worker's job- or job-related experiences (Locke, 1976). In Figure 3, *organizational commitment* and *continuance commitment* are two main outcomes of technostress and they are both parallel to organizational outcomes in Figure 2. Organizational commitment means how strongly an individual identifies with and is involved in a particular organization (Porter, Steers, Mowday & Boulian, (1974). Continuance commitment refers to a situation where a worker views that they gain more by staying in an organization than they lose (Shore & Wayne, 1993, Eslami & Gharakhani, 2012). Previous study on stress has shown that strains lead to reduced organizational commitment (Beehr, 1998). A bulk of previous studies have also shown evidence that job satisfaction positively affects individuals' organizational commitment (Al-Aameri, 2000; Cheloha & Farr, 1980, Rabinowitz & Hall, 1997 as cited in Ragu-Nathan et al. 2008).

A factor that is unique to Figure 3 without a parallel factor in Figure 2 is *Individual differences*. Ragu-Nathan et al. (2008) argues that there are four characteristics that affect how an individual experiences technostress. These characteristics are *age*, *gender*, *education*, and *computer confidence*. These characteristics have been chosen for the model for several reasons. Previous studies have shown that education positively affects an individual's perceived ease of use of ICTs, and it shows that more educated users experience less anxiety and learn new ICTs faster than users with less education (Igbaria & Parsuraman, 1989, Agarwal & Prasad, 1999, as cited in Ragu-Nathan et al., 2008). However, there are significant differences in previous studies on how age affects the use of information technology. Typically, older people are unenthusiastic about learning new technologies (Charness & Boot, 2009). Previous studies also found that ICT ease of use is

negatively affected by age (Burton-Jones & Hubona, 2005). Interestingly, studies on computer and stress found that age has no impact on computer phobia and a "computer phobic" can be young or old and male or female (Rosen & Maguire, 1990). Studies on technostress has found that age does have an effect on technostress (Ragu-Nathan et al., 2008).

When it comes to gender, studies have shown that that different factors influence men's and women's use of ICT. Men seems to be more likely to use computers in workplaces and they are less influenced by subjective norms in an organizational environment (Venkatesh & Morris, 2000). Men also find software easier to use than women (Gefe & Straub, 1997). Additionally, women seem to experience higher levels computer anxiety (Igbaria & Chakrabarti, 1990, Whitley, 1997, as cited in Ragu-Nathan et al., 2008). Studies have also found that women seem to be slightly more computer phobic than men (Rosen & Maguire, 1990). Interestingly, despite these findings, studies have found that men seem to experience more technostress than women (Ragu-Nathan et al., 2008, Jena & Mahanti, 2014).

It is very important to understand technostress as the help of ICTs can aid users in repetitive tasks and allows them to create new working techniques, use time more efficiently and improve their technological skills, but these benefits can coexist with feelings of frustration and distress (Brod, 1984, Hudiburg, 1989, as cited in Ragu-Nathan et al., 2008).

3.3 Technostress creators

Technostress creators are at the core of this thesis when it comes to understanding if password managers cause their users to experience technostress. There are many proposed and studied categories of technostress creators in recent technostress research, but the five categories suggested by Tarafdar et al. (2007) are the most widely studied and acknowledged. These five categories of technostress creators are: *techno-overload*, *techno-invasion*, *techno-complexity*, *techno-insecurity*, and *techno uncertainty*. These are the key factors in technostress literature that influence how technostress is formed.

Techno-overload refers to user experiencing too many encounters with information and technological functions. This includes situations where use of ICTs forces users to work a lot faster and longer (Tarafdar et al., 2007). It refers to a point where users are expected to accomplish more than it is possible, and it measures how much use of ICT forces its users to work more. (Harris, Harris, Valle, Carlson, Carlson, Zivnuska & Willey, 2022). Techno-overload is connected with situations that creates stress and forces users to work faster and longer than normal and has a potential to lead to fatigue, memory challenges and loss of control in workers (Ingusci, Signore, Giancaspro, Manuti, Molino, Russo & Cortese, 2021). Techno-overload can be seen being the overlap between technostress and work-overload (Thurik, Benzari, Fisch, Mukerjee & Torrès, 2023). While a

password manager might be an additional burden for their users to learn and might force users to work harder, it might also alleviate some of the experienced technostress by reducing the burden of remembering different passwords. Therefore, it is hypothesized that:

H2: There will a difference in techno-overload between password manager users and non-users.

Techno-invasion refers to excessive technology intruding into the user's life. User may feel that technology invades major parts of their lives, creating a feel of stress. The use of ICT can create a situation where its users can be reached anytime and users might feel that they must always remain connected to, for example, work related networks and always be available (Ragu-Nathan et al., 2007). In work related environments, ICT usage in free time can create a feeling of being exposed to the ICT and forces them to stay connected to work, even at home (Tarafdar, Ragu-Nathan & Ragu-Nathan, 2011). Mobile password managers follow users everywhere, but having access to all passwords anywhere can also be relieving. Therefore, it is hypothesized that:

H3: There will be a difference in techno-invasion between password manager users and non-users.

Techno-complexity refers to difficulty to use technology. It is related to the difficulty to learn new technologies and feeling of not being adept enough to use the associated technology while forcing individuals to invest more of their time and effort in order to understand them and learning to use them effectively (Tarafdar et al., 2007; Ragu-Nathan et al., 2008). Many password manager users consider that using a password manager is easy and makes remembering password managers easier, while many of the non-users expresses their considerations towards them by saying that they seem inconvenient, or they do not have the time to learn to use them (Fagan et al., 2017). Therefore, it is hypothesized that:

H4: There will be a difference in techno-complexity between password manager users and non-users.

Techno-insecurity is referring to situations where users are fearful of losing their jobs because of their inability to use a technology (Tarafdar et al, 2007). An employee can feel that co-workers that are more capable to use a technology threatens their position their organization (Ragu-Nathan et al., 2008). They may feel pressured to constantly update their ability to use this technology in order feel more secured and may experience a fear of being replaced which may also cause them to not share their knowledge with co-workers (Tarafdar et al, 2007). *Techno-uncertainty* refers to a feeling of uncertainty that a user may feel because of constant evolution of technology and which problems this may cause to the

individual later (Ragu-Nathan et al, 2008). User may be stressing that their hard work towards learning a technology may be rendered invalid by a newer replacing technology (Tarafdar et al., 2011). Users may initially be passionate about learning new technologies but constant updates and requirement to re-learn technology related tasks may create a feeling of anxiety and frustration (Tarafdar et al., 2011). Some evidence indicates that changes in password managers may steer users away from using password managers (Ray, Wolf, Kuber & Aviv, 2021). However, updates for the better can make password manager usage easier and less stressful. Therefore, it is hypothesized that:

H5: There will be a difference in techno-uncertainty between password manager users and non-users.

Out of these technostress creators most relevant to password managers and why users might not use them is techno-complexity and to some degree techno-invasion. One suggested hypothesis is that potential is already using excessive amount of ICT and different software and learning to use a password manager does not feel like an attractive trade-off to do. On the other hand, some users might find password managers too difficult to use over more traditional methods, such as typing passwords down to a post-it note.

These five technostress creators are the most acknowledged causes of technostress, and this study will be examining four of them, excluding techno-insecurity, which is not applicable to password manager context. It is, however, important to acknowledge that more recent studies have found more than the five categories proposed by Tarafdar et al. (2007). Ayyagari, Grover & Purvis (2011) proposed five more categories of technostress creators. These categories are *work overload, role ambiguity, invasion of privacy, work-home conflict,* and *job insecurity*. It is worth noting that as technostress research progresses new categories of technostress are proposed at a rather frequent rate and many of them are derived from existing stress research.

Work overload means that assigned task exceeds a worker's capability or level of skill. Workload can be either quantitative or qualitative, where former refers to a concrete amount of work required within a time frame and the latter refers to a situation where an individual believe that they do not possess the required skill or capacity to perform their job and is connected to low self-esteem (Cooper, Dewe & O'Driscoll, 2001). *Role ambiguity* refers to the uncertainty regarding the outcomes of fulfilling a particular role and a lack of necessary information to effectively carry out that role or simply lack of clarity of an individual's role (Kahn, Wolfe, Quinn, Snoek & Rosenthal, 1964 as cited in Cooper et al., 2001). For example, many individuals tend to keep their email open or set up notifications on their mobile phones to promptly address incoming emails. However, the constant pressure to be present and responsive can end up consuming valuable work time. The interruptions generated by these demands introduce uncertainty regarding which task or job should be prioritized, thereby limiting an individual's abilities. Moreover, ICTs enable multitasking, which adds an additional layer

of decision-making as individuals must determine which tasks to undertake and in what specific order. (Ayyagari et al., 2011.)

Invasion of privacy refers to individual's perception of his personal privacy being compromised (Alge, 2001; Eddy et al., 1999 as cited in Ayyagari et al., 2011). Feeling of being constantly connected by ICTs can create feeling of strain and stress. Sometimes individuals might have a feeling that they are required to remain connected to work. *Work-home conflict* refers to a situation where work and private life are intertwined due to ICT usage (Galvin, Evans, Nelson, Richards, Mavritsaki, Giovazolias, Koutra, Mellor, Zurlo, Smith & Vallone, 2022). *Job insecurity* means a situation where an individual feels their job or career is threatened (Ayyagari et al., 2011).

3.4 Technostress effects

Technostress has been found to have a considerable effect on both organizational and individual level. There has been a good bulk of recent studies examining how technostress impacts an individual. ICT usage in organizational environment has been increasingly resulting in negative effects in employees, such as information overload and interruptions (Tarafdar et al. 2016). Brod (1984) interviewed people in multiple organizational levels and on different phases of ICT adaption and found very easily recognizable stress symptoms such as fatigue and headache. In addition to that, Brod found that workers were internalizing the standards in which the computer operates: accelerated perception of time, perfectionism, and a binary "yes-no" way of thinking. Technostress also has been found to cause negative effects on performance, and if organization fails to manage ICT-related stress in their workers, technostress can negate the increases in productivity offered by the used new technology (Tarafdar et al., 2007). Previous study has shown technostress to result in work overload, frustration, information exhaustion, low motivation levels, and general work dissatisfaction (Ragu-Nathan et al., 2008). It has been found that technostress significantly reduces employees' well-being and on the other hand technostress inhibitors can significantly improve their well-being (Hang, Hussain, Amin & Abdullah, 2022).

In educational environment, technostress seems to decrease academic productivity in university students (Upadhyaya & Vrinda, 2021). Technostress has shown to aggravate role overload, reduce job satisfaction, decrease innovation in tasks, reduce productivity and reduce organizational commitment and workers who experience technostress are less satisfied with their jobs and their ability to use information systems in their tasks is diminished (Tarafdar et al., 2011). Technostress is associated with a number of consequences in organizational environment, such as work dissatisfaction, worse productivity, increased job-related depression and anxiety, as well as exhaustion and burnouts (Tarafdar et al., 2020). Mobile devices, social networking and different team collaboration tools may together force users to process massive amount of information which

can result in interruptions, information overload and multitasking (Tarafdar et al., 2011).

Newer studies argue that technostress has both positives and negatives, and stress caused by the use of ICT may even be positive (Califf, Sarker & Sarker, 2020). Studies argue that many of the technostress creators are liked to both negative and positive responses and such responses are related to job satisfaction and attrition (Califf et al., 2020). Technostress creators have been found also to have positive impact on job outcomes if the individual possess certain personality traits (Srivastava, Chandra & Shirish, 2015).

Currently there is not a great volume of studies that have been able to prove direct correlations between mental disorders and technostress. There are, however, studies that report use of digital technologies associated with certain psychological demands resulting in stress reactions. Empirical studies on technostress and mental health are often small in sample size and lack longevity. They also may not always have proper measures for psychological strain. Majority of the few studies that study technostressors are focused on ICT associated with burnouts. These studies suggests that workers should be able to "disconnect" after work to reduce the risk of burnout. There are also studies that measure industrial robots associated with metal health and they showed a decrease in mental health when robot intensity (employee to industrial robot ratio) was higher. (Dragano & Lunau, 2020)

4 METHOD

This chapter discusses the research methodology, commencing with the presentation of participant data, followed by an analysis of survey findings. Lastly, there will be a discussion of the procedure.

4.1 Participants

306 participants were recruited to take part in the survey. The participants had a range of ages with the largest group being 36-45 years old with 105 respondents. The second largest group was 26-35 years old with 98 respondents. A majority of respondents with 174 (56,9%) responses reported their gender as male and 131 (42,8%) reported their gender as female. One single respondent reported their gender as other, and two respondents wished not to report their genders. The majority of respondents with 157 (51,3%) responses reported their education as a bachelor's degree or an equivalent qualification. Second largest educational groups were people with highschool education (or equivalent) and people with master's degree or equivalent with 67 (21,9%) responses each group.

The respondents were divided into two groups based on if they are currently using a password manager or not. Out of 306 responses 202 (66,0%) reported that they are currently using some kind of password manager and 104 (34,0%) reported that they are currently not using any kind of password manager.

Table 1: Respondents' age, gender, and education distribution

Age	N	%	Gender			Education	N	%
25 or under	16	5,2 %	Male	172	56,2 %	High school education	67	21,9 %
26-35	98	32,0 %	Female	131	42,8 %	Bachelor's Degree/Undergraduate	157	51,3 %

36-45	105	34,3 %	Other	1	0,3 %	Master's Degree/Graduate	67	21,9 %
46-55	52	17,0 %	Prefer not to say	2	0,7 %	Doctorate Degree	6	2,0 %
56 or older	35	11,4 %				Other	9	2,9 %
Total	306	100,0 %						

4.2 Measures

This study is conducted as a survey. Survey is a method to systematically collect information about or from people to compare, describe or explain their attitude, knowledge, and behaviour (Fink, 2003). A survey study was the chosen method as it is, with right tools, a straightforward and reliable method to measure desired factors.

A Likert Scale of 1 to 5 was used for the survey, as it is one of the most commonly used self-report measurements to measure unobservable constructs (Jebb & Tay, 2021). The survey questions are mostly quantitative, having questions about respondent background including age, gender, education, and clarifying questions regarding the individual's current password manager usage. The final question of the survey is an optional open-text field question where respondent can choose to tell why he uses or does not use a password manager. An open-text field question was included to enrich the data and to receive more insight from different perspectives. This option was added to get some optional insight to the answers and to see if there are trends among respondents' opinions. The main goal of the survey is to measure four of the five technostress creators presented by Tarafdar et al. (2007), as these technostress creators are the most widely acknowledged and studied. The survey aims to measure:

- *Techno-overload*. The survey aims to measure, whether password managers cause individuals to experience increased workload, put more effort and have less time for other things.

- *Techno-invasion*. Do password managers cause individuals to feel that password managers invade their personal lives?

- *Techno-complexity*. Are password managers too complex and time consuming for individuals to learn and use?

- *Techno-uncertainty*. Do password managers cause individuals feelings of uncertainty and lack of constancy?

Out of the five technostress creator categories presented by Tarafdar et al. (2007), techno-insecurity was chosen to be left out. Techno-insecurity is mostly

associated with work environments and fear of losing one's job, which is not relevant or realistic situation when considering a password manager usage. At the very least it is a rather specific topic to measure an individual's fear of losing his or her job because of using or not using a password manager. For these reasons and to keep the scope reasonable, techno-insecurity was left out of this study.

This survey had three questions to measure each of the technostress creators and most of the questions were slightly or moderately modified questions adopted from a study by Tarafdar et al. (2007). For example, the question 14 "I find password managers too complex for me to use and understand" aims to measure techno-complexity. The corresponding question in the study by Tarafdar et al. (2007) is "I often find it too complex for me to understand and use new technologies". The Cronbach Alpha analysis was conducted for the pilot study questions and responses, and all Cronbach's Alpha values exceeded 0,7, indicating the suitability to proceed with the main study.

Table 2: Survey questions measuring technostress creators and their corresponding questions by Tarafdar et al. (2007)

Measured factor	Survey questions	Original questions	Cronbach's Alpha
Techno-overload	I would be forced to use more effort than I can handle when using a password manager	I am forced by this technology to do more work than I can handle	0,856
	By using a password manager, I would have less time for other things	I am forced by this technology to work much faster	
	Using a password manager would increase my workload	I have a higher workload because of increased technology complexity	
Techno-invasion	I feel that using a password manager would cause me to have less time for other important things in my life	I spend less time with my family due to this technology.	0,862
	I feel that using a password manager would invade other parts of my life	I feel my personal life is being invaded by this technology	
	I feel that I have to sacrifice my vacation and weekend time to use password manager efficiently	I have to sacrifice my vacation and weekend time to keep current on new technologies.	

	I feel that I do not know enough about password managers to use them effectively	I do not know enough about this technology to handle my job satisfactorily.	
Techno-complexity	I do not find enough time to learn to use password managers	I do not find enough time to study and upgrade my technology skills.	0,848
	I find password managers too complex for me to use and understand	I often find it too complex for me to understand and use new technologies.	
	I feel that password managers receiving constant updates makes their usage difficult		
Techno-uncertainty	I feel that password managers are constantly changing	There are constant changes in computer hardware in our organization.	0,862
	I feel that password managers are frequently receiving updates	There are frequent upgrades in computer networks in our organization.	

A Confirmatory Factor Analysis (CFA) was run in AMOS for survey factors. The Cronbach Alpha was calculated by using SPSS and the results showed that the technostress creator factors were reliable by the Cronbach's Alpha exceeding 0,7 (Nunnally, 1978). Cronbach's Alpha values for each factor are listed in Table 2. Factor loadings and factor correlations were at adequate levels, as all factor loadings exceeded value of 0,60 and none of factor correlations exceeded 0,80. The model fit was at good levels without any need to do changes to the model. The Standardized Root Mean Square Residual was found sufficient at 0,046 when anything below 0,1 indicates a sufficient fit. Value for the Comparative Fit Index (CFI) was 0,960 which also indicates a good level of fit. Tucker-Lewis Index was sufficient at 0,944 being close to cutoff value of 0,9. Root Mean Squared Error of of Approximation (RMSEA) value was 0,084 which deviates from recommended RMSEA cutoff value of 0,6 but because SRMR, CFI and TLI were at sufficient levels of fit, it can be concluded that the model works and is correctly measuring desired factors despite suboptimal RMSEA value. (Hu & Bentler, 1999)

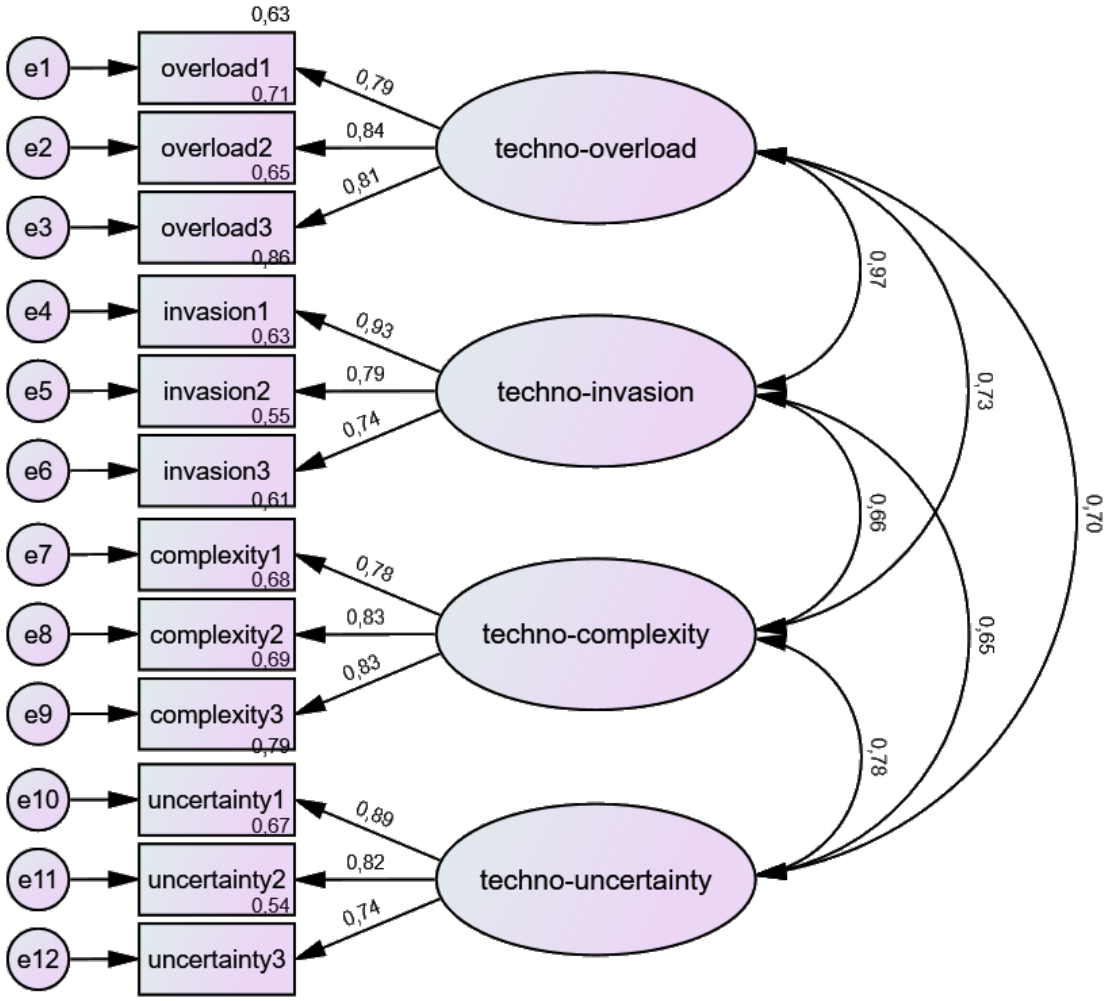

Figure 4: Measurement model for standardized factor loadings and factor correlations

4.3 Procedure

Before sending out the main surveys, a pilot survey was conducted to test that the survey is functioning and measures desired factors. The pilot survey received 23 responses and some translation corrections were made for the main survey to ensure that the same questions in English and Finnish are as accurate as possible.

The data was collected via two online surveys. The first survey was shared via University of Jyväskylä IT faculty email list and different social media platforms, such as Facebook, LinkedIn, and Discord. The respondents were volunteers who were willing to participate in the survey. The first survey received 101 responses. The second survey was conducted via Amazon MTurk which gathered 205 responses totalling 306 individual responses, which exceeds threshold of 100 which is the minimum number of responses for a study that aims to use factor analysis (Kotrlik & Higgins, 2001).

All messages leading to the surveys provided information of the respondents' responses being handled anonymously and confidentially. The same

information would also be provided on the first page of the survey. Respondents were also informed that all answers would be anonymized, and their responses could not be linked back to them. The respondents were also informed that the estimated time to complete the survey was up to 5 minutes. The survey data were collected with two separate online surveys. The survey was conducted in entirety with survey software Webropol.

The Finnish translation of the survey was done by two native Finnish speakers by translating them from the English questions. After being approved by both translators, the Finnish questions were included to the pilot study and to the main study. After the surveys were completed, the response data was combined in SPSS software. The written open questions were categorized and will be further examined in results.

5 RESULTS

Data from 306 responses were analysed to examine any causal relationship between password managers and technostress. Independent Samples T-Test was used to observe statistical differences between password manager users and non-users. The analysis and categorization of open questions will also be done.

5.1 Technostress levels between password manager users and non-users

To test if we can reject null hypothesis for password manager users and non-users, Independent Samples T-test was applied to the sample to observe potential differences between password manager users and non-users. Test was applied to each of the measured factors and to overall experienced technostress. Equal variances were observed in all measured factor groups, except for techno-complexity, in which Levene's Test for Equality of Variances showed significance value of <000,1 and null hypothesis was rejected. In other factor groups, Levene's Test showed significance value of greater than 0,05 and null hypothesis was accepted on those groups. T-test results can be observed in Table 4.

Table 3: The T-test results comparing technostress between password manager users and non-users.

	Users (N = 202)		**Non-users (N = 104)**					
	M	**SD**	**M**	**SD**	**Mean difference**	***t***	**df**	**Sig (2-tailed)**
Technostress	1,71	0,79	2,27	0,82	-0,56	-5,84	304	<0,001
Techno-overload	1,70	0,99	2,21	1,03	-0,51	-4,22	304	<0,001

Techno-invasion	1,48	0,86	1,76	0,91	-0,28	-2,63	304	0,009
Techno-complexity*	1,69	0,90	2,47	1,15	-0,78	-6,02	170	<0,001
Techno-uncertainty	1,95	0,90	2,64	1,01	-0,69	-6,10	304	<0,001

**Equal variances not assumed by Levene's Test*

The findings suggests that overall technostress is higher among the non-user group. The mean for non-user respondents is much higher with a statistically significant p-values, which suggests that overall experienced technostress is higher among all measured factors.

There are some differences in how much the two groups differ among the factor groups. The t-test shows that there is no statistical difference in variance between users and non-users, but the difference in mean is highly statistically significant. In techno-invasion the mean difference is much smaller than in other measured factor groups, but two-tailed significance is still below the value of 0,05 which suggests high level of significance in differences in means. It shows that the t-test indicates high level of significance in differences, but in a lesser degree than other factor groups. Techno-complexity was interestingly the only factor where null hypothesis for equal variances could be rejected based on Levene's test but was also showing high level of statistical significance with two-tailed p-value being <0,001. Techno-uncertainty was similar to techno-overload in terms of T-test results as it also showed high difference in means, similar variances, and high levels of statistical significance.

In this thesis, five hypotheses (H1 – H5) were formulated to explore differences in technostress levels between password manager users and non-users. Looking at the first hypothesis, "*There will be a difference in technostress between password manager users and non-users,*" it can be noticed that measured technostress is different in password manager users and non-users (t = -5.84, df = 304, p < 0.001, two-tailed), supporting H1. In the second hypothesis, "*There will a difference in techno-overload between password manager users and non-user*" it can be noticed that measured techno-overload levels are different between users and non-users (t = -4.22, df = 304, p < 0.001, two-tailed). Therefore, H2 is supported. The third hypothesis "*There will be a difference in techno-invasion between password manager users and non-users*" is likewise supported. It can be noticed that there is a difference between users and non-users in techno-invasion (t = -2,63, df = 304, p = 0.009, two-tailed), supporting H3. In the fourth hypothesis, "*There will be a difference in techno-complexity between password manager users and non-users*" we can also notice that password manager users and non-users have a difference in techno-complexity (t = -6.02, df = 170, p < 0.001, two-tailed). Like others before, hypothesis is supported. Finally, with the fifth hypothesis "*There will be a difference in techno-uncertainty between password manager users and non-users*" it can also be noticed that password manager users and non-users have a difference in

techno-uncertainty (t = -6.10, df = 304, p < 0.001, two-tailed). Therefore, H5 is supported.

Table 4: The hypotheses and whether they are supported.

Hypothesis	Supported
H1: There will be a difference in technostress between password manager users and non-users.	Yes
H2: There will a difference in techno-overload between password manager users and non-users.	Yes
H3: There will be a difference in techno-invasion between password manager users and non-users.	Yes
H4: There will be a difference in techno-complexity between password manager users and non-users.	Yes
H5: There will be a difference in techno-uncertainty between password manager users and non-users.	Yes

5.2 Analysing of open question responses

After thoroughly reviewing all written responses, the responses were categorized based on reoccurring themes regarding password manager usage. Each respondent received an optional open question at the end of the survey based on the first question "Are you currently using a password manager?". The open questions were "Why do you use password managers?" and "Why do you not use password managers?". User and non-user responses were reviewed separately and were categorized. For users, nine distinct reasons to use password managers were identified: password memorability, password security, convenience, easier password management, external pressure, peace of mind, credential access, time saving and other. For non-users, ten different reasons to not use a password manager were identified: distrust, lack of need, reluctance, other, difficulty to learn, inconvenience, lack of time, inactivity, and lack of knowledge. These findings align well with previous studies and the reasonings to use or not use a password manager are similar to existing study by Fagan et al (2017). A good number of open question responses were received: 192 from password manager users and 101 from non-users, totalling 293 open question responses, which is 95,8% of all survey responses.

Table 5: Respondents' reasons for using or not using a password manager.

Users			Non-users		
Category	**N**	**%**	**Category**	**N**	**%**
Password Memorability	61	31,8 %	Distrust	38	37,6 %
Password Security	47	24,5 %	Lack of Need	26	25,7 %
Convenience	33	17,2 %	Other	16	15,8 %
Easier Password Management	33	17,2 %	Inactivity	12	11,9 %
Other	18	9,4 %	Reluctance	9	8,9 %
User responses	**192**		**Non-user responses**	**101**	

Starting with the users, a majority of them reported that their main reasons to use a password manager is to make it easier to remember passwords. 61 of password manager users reported that their primary reason to use a password manager is to alleviate the burden of remembering long and secure passwords. One respondent thought that they would likely just re-use passwords without the aid of password manager.

> "I believe that with a password manager, I can free up brain capacity (memory) for more useful tasks. I don't have to remember passwords, and on the other hand, with the help of the management software, I can create secure and as strong as possible passwords for necessary purposes. Without the password manager, I would likely use the same password or at least easily derived passwords, which certainly does not increase security." (Translated from Finnish)

While not having to remember passwords is the main reason to use a password manager, one respondent acknowledged usefulness of password managers' security notifications if a password is compromised or leaked online.

> "So that I wouldn't have to remember all my passwords and I also receive security notifications if, for example, a password has been compromised or if I accidentally use the same password for different services." (Translated from Finnish)

Interestingly, one respondent found that not having to remember passwords is helpful because of memory issues caused by medication.

> "My epilepsy medication causes me to have memory issues. Using them is extremely helpful since I am online all day on many different sites."

A common theme among open question responses seems to be that secure passwords are difficult to remember, and it is where a password manager comes in handy. Respondents seem to have a real interest in having a strong password.

> "I got tired of trying to create my own passwords and remember all the different little changes I would make. There's way too many things to remember, and what I can remember doesn't make a great password."

The second largest group of password manager users reported that their primary reason to use a password manager is related to password security. These respondents primarily wanted to have a strong password and a password manager was in many cases the best way to achieve this. A respondent valuing personal security had some distrust in external password managers but opted to save their passwords locally.

> "I use the browser's built-in password manager, which stores passwords locally. I don't trust external services, and I have a more negative opinion of them. I mainly use the password manager to create strong passwords, and of course, the fact that I don't have to remember the password myself makes life easier." (Translated from Finnish)

A common theme among people in this group expressed their concerns about securely using a large number of credentials without compromising their password information. Following respondent also appreciated that with a password manager you can access your credentials on their phone.

> "I like having unique passwords for all my accounts and with over 100 accounts it's too difficult to remember them. I also like having a password manager with an app, so I have access to my passwords on my phone."

Among the responses there were also some appreciations toward password managers' password generation features.

> "To help keep my passwords safe. It also allows me to use "suggested passwords" that are very complicated without me having to remember them."

> "It has multi-platform support that helps to generate strong password and high security options along with easy recovery options."

> "I think that using a password manager makes my online accounts more secure, because I now use only randomly generated, longer passwords for all of my logins. If I wasn't using a password manager, I wouldn't be able to use these more secure passwords because it would be too difficult for me to remember them all. In addition, I use a password manager because it's faster and easier for me."

Many respondents mainly used password managers because they are convenient. There were multiple ways in which the users considered password managers convenient. For example, a respondent said that browser-integrated password manager just makes everything easier and faster.

> "It's too easy not to use the browser's built-in password manager. Everything happens automatically. All other methods would require more work than manually typing them into a separately installed password management software specialized for that purpose." (Translated from Finnish)

Many respondents mentioned that they appreciate password management software for speeding up their work or simplifying login to various services.

> "They significantly speed up the work at my workplace." (Translated from Finnish)

> "It makes everything easier when it comes to anything that's behind a password." (Translated from Finnish)

> "It simplifies my life. I used to keep passwords in notes, or handwritten notes, this way they get added for me."

A respondent also appreciated browser-integrated password managers and considered them a better option than manually noting down passwords.

> "I only use the password manager integrated in my browser, the one that gives a message/option 'do you want to save this password?' I use this tool because it is part of my browser already and I don't have to install anything. It helps because I am tired of trying to save passwords on an index card by my computer, which isn't really safer anyway."

Easier Password Management was also a rather popular reason to use password mangers. While responses were similar to Convenience, in this category the respondents expressed their appreciation towards password mangers' ability to make managing multiple credentials even possible instead of being a convenient tool.

> "There's no reason not to use it. Currently, I use Bitwarden software on my mobile, desktop, and browser. My BW database currently contains over 700 unique secrets. It cannot be managed in any other way than with password management software." (Translated from Finnish)

> "The only realistic way to use a different password in different places." (Translated from Finnish)

> "Password managers greatly simplifies everyday life because I have so many user accounts for various services. Using the software reduces my mental load because I don't have to remember tens of different passwords. I feel more secure when I have a long, unique password for all of my services." (Translated from Finnish)

Few users started to use password manager because of some external pressure. For instance, some workplaces require their employees to use them.

> "The company I work for mandates their use. Later on, I started using a password management software in my personal life to enhance my security with unique and strong passwords for various services." (Translated from Finnish)

> "Many websites (such as universities), now require extremely strong passwords (with a character count exceeding 16 and special characters). Creating such passwords manually is very difficult, let alone remembering them, which is why password management software is almost mandatory." (Translated from Finnish)

> "My spouse strongly encouraged me." (Translated from Finnish)

Interestingly, one user mentioned using password managers to ease online payments.

> I have a lot of online bills. All have different passwords. It is easier to use a password manager in order to pay my bills.

In the non-user side, the biggest reason to not use a password manager is Distrust. These concerns primarily stem from the fact that all passwords are stored in one location, raising concerns about the potential compromise of all their credentials and the vast majority of these responses were concerned about that. There were different concerns as well, for instance, regarding losing access to all credentials if the master password is forgotten.

> “It centralizes control over everything. It's unwise.”

> “The last time I used one, I got hacked and all my passwords were taken. So I just manually write them down in a book now.”

> “Have more trust just remembering passwords on my own. Plus, just never bothered to use one. If I get used to using a manager then end up forgetting my passwords, if I am somehow blocked from my manager I am screwed.”

> “I don't like the idea of having all my passwords in one place. Doesn't seem safe.”

The second largest group of reasons to not use password managers was Lack of Need. A large number of respondents simply doesn’t have a need for password managers and believe that they can manage their credentials without. A recent breach to a certain password manager also raised some concerns.

> “I have a system I use and don't feel I need a password manager, plus the Lastpass breach makes me nervous about using one.”

> “It doesn't really seem necessary to me and I'm able to keep track of my passwords.”

One respondent chooses to use a simple set of memorable passwords instead of password manager.

> “I don't have a very diverse set of passwords in use. So I can fairly easily remember my current passwords mentally.”

Interestingly, the third largest group of non-users reported that they are not using password managers simply due to laziness or not being active enough to start using them.

> "I have never had the energy to delve into the whole thing. I know they exist, but I am not so interested that I'd put in the effort. Maybe I will take a look at them someday." (Translated from Finnish)

> "I haven't been able to start using it, even though I know I should." (Translated from Finnish)

> "I just have a school of fish philosophy when it comes to internet security and find it simply not worth the time and effort to cover the small amount of risk it carries. That and admittedly I'm not a very disciplined person. It's also laziness on my end for sure."

> "I have not actively searched, and I haven't come across a good one. In other words, I may not be aware of the benefits of the program." (Translated from Finnish)

Nine non-users were reluctant to use password managers, reasonings ranging from discomfort to adoption barrier.

> "The threshold for learning and adoption has been high. Additionally, it would require finding out which of the different password manager options is the most suitable." (Translated from Finnish)

> "I do not use them because I just never have tried, and don't like having my passwords stored in something, it just scares me a bit."

> "I prefer to manage passwords on my own, without having to rely upon a third party. I also worry that if I somehow lose access to the password manager by not being able to log into their system, I will be unable to access any of my accounts. I'd rather have each password be separate, so that forgetting one password or login won't prevent me from accessing my other accounts."

The non-users provided some responses that were more difficult to categorize, categorizing 4 of them in the "other" category. One respondent stated that they had never heard of password managers.

> "I've never heard of it."

One respondent admitted that inadequate safety habits are the reason for not using a password manager.

> "I have bad internet safety habits and use the same password for everything."

Three respondents lacked the knowledge of password manager functionalities and features, which they reported being the main reason for not using a password manager.

> "I'm concerned about compatibility across different computers. Maybe this is un-founded. I don't really know a great deal about them."

> "I don't know anything about them to use them."

Three non-users reported not having enough time to use a password manager.

> "I don't use them because there are too many of them to learn more about them. It's hard to dedicate time to research which ones are reliable to use and how to use them."

And finally, three non-users thought that password managers are inconvenient.

> "I found in the past that it was more trouble than it was worth. Also, I don't trust them."

Many opinions about password managers were in common between categories. For example, a huge number of users appreciated all benefits of password managers, such as easier password management, and increased security, but the responses were still put into only one category per response. Realistically, based on these responses, it seems likely that password manager users are generally well versed in benefits of password managers and use them because of their combined benefits. Non-user responses on the other hand were slightly more homogenic and focused on specific problem rather than listing multiple problems. However, it is worth nothing that many given major categories to not use password managers cannot be strictly tied to different technostress creators. For example, Lack of Need hardly qualifies as an indicator of technostress.

To summarize, password manager users mostly reported using password managers because of password memorability, password security, convenience or to ease password management. Of all password manager users who responded to open question, 90,6% falls into one of these categories. The non-users primarily opted not to use password managers because of distrust, lack of need, inactivity, or reluctance, with 84,2% of responses falling into these categories.

6 DISCUSSION

The purpose of this chapter is to discuss the findings, research questions, limitations, and reflect these on existing literature. Some practical implications for the findings will be discussed as well.

6.1 Difference in technostress

This thesis explored the differences in technostress levels between password manager users and non-users. Using data collected with a survey, responses from 306 respondents were analyzed and it was found that password manager non-users seem to experience statistically significantly higher levels of technostress in four measured areas of technostress, also known as technostress creators: techno-overload, techno-invasion, techno-complexity, and techno uncertainty. Previous studies have indicated that intensive users of technology experience technostress to a lesser extent compared to non-intensive users (Salanova et al., 2013) and findings in this study are aligned with this. The survey validity is good as the number of respondents were high (N=306) and the respondent group was highly heterogeneous.

Confirmatory Factor Analysis showed good model fit and proposed model showed good model fit with both groups. The model required no further adjustments. Good model fit indicates that the survey correctly measures technostress and survey results show that both users and non-users experience some levels of technostress. This answers affirmatively to the first research question: "Do password managers cause technostress?". Independent Samples T-test was conducted to examine differences between users and non-users and statistically significant differences were found, which answers affirmatively to the second research question: "Is there a difference between in technostress levels between password manager users and non-users?". Confirmatory Factor Analysis is a widely used method to test models based on theoretical frameworks and

Independent Samples T-Test is a widely used method to compare two groups, and they both contribute to validity of this study.

Open questions offered some additional insight to minds of users and non-users indicating that there are a variety of reasons to use or not use password managers and showed that main reasons to use password managers are password memorability, password security, convenience, and easier password management. Given main reasons to not use password managers are distrust, lack of need, inactivity, and reluctance.

6.2 Contribution and practical implications

The results of this thesis contributed to technostress and password manager research greatly as there is currently no existing literature of measuring technostress caused by password managers. There are, however, studies that measure technostress on users and non-users but not in the context of password managers. There are also studies that explore reasons for using password managers (Oesch et al., 2022; Pearman et al., 2019). The open question responses contributed to repeatability of existing password manager literature about reasons to use or not use password managers and received similar results.

Understanding that password managers can cause technostress has practical implications. This awareness can assist password manager developers in improving their software to alleviate technostress-related issues. Addressing these problems can help remove barriers to entry for some users. Because password managers are found to generally increase password security (Luevanos et al., 2017), larger number of people having a password manager would result in less security breaches. Security breaches in organizational environments are even more severe than for individual people (Arias-Cabarcos et al., 2016), which means that understanding password managers' potential to cause technostress could save companies from financial or reputational damage. Having fewer stressors in organization can also increase worker productivity and well-being while reducing stress and feeling of overload (Ragu-Nathan et al., 2008). It is also worth noting that survey indicates that distrust towards external password managers a major concern among password manager non-users. Improving trust toward password managers could be a good first step towards better and less technostress-causing password management software.

6.3 Limitations and future research

This thesis also had some limitations which should be discussed. First, this study did not dive very deep into various areas of technostress and technostress creators. Only four of the five most studied and acknowledged technostress creators proposed by Tarafdar et al. (2007) were used and other newer areas of

technostress were generally ignored. This leaves room for speculation of which areas of technostress are the most prominent in password manager context. Also, possible underlying factors were not explored. It should also be noted that even though responses from open questions align well with existing literature, no strong conclusions should be made from these as they were not the main scope of this study.

This thesis suggests technostress may be one of the main reasons why many people choose not to use password managers, which is why this topic deserves to be studied in greater detail. This thesis measured technostress at a very general level and did not much into specifics as why do password managers cause technostress which is one of the possible frontiers for future research. As new research emerges new potential technostress creators, future research has the opportunity to delve deeper into various sectors of technostress. Specifically, it can investigate which stressors play the most significant roles in the context of password managers. Another possible domain for further research could be to examine technostress levels inside different groups, such as elderly people or people with varying levels of ICT experience. Another possibility for future research would be to focus on specific types of password managers, such as mobile apps or desktop applications. Further research could help to improve password managers which, in turn, would result in increased personal security for a larger number of people.

7 CONCULSION

The purpose of this thesis was to find out if password managers cause technostress and whether there is a difference in technostress levels between users and non-users. Understanding password managers and their potential to cause technostress can help password manager providers to improve their software to alleviate potential technostressors in their products.

There is no prior research measuring technostress caused by password managers which is why this thesis offers new insight to existing technostress and password manager research. When it comes to previous research on ICT usage and technostress, studies have shown that people who use certain ICT frequently experience less technostress than users who use them less frequently (Salanova et al., 2013). Previous research also points out that increasing number of people is seeking alleviation to burden of remembering many complicated passwords and password managers are a frequently proposed answer (Li et al., 2014). Past studies also show that even though password managers are frequently recommended by many experts, they are not very widely used (Fagan et al., 2017). This thesis tried to uncover some of these unexplored areas of technostress and password manager research to shed light on why some people are reluctant to use them.

The results suggest that password managers can cause technostress in both users and non-users. The results also suggest that password managers cause non-users to experience significantly higher levels of technostress across all four measured areas of technostress: techno-overload, techno-invasion, techno-complexity, and techno-uncertainty. These technostressors are based on five technostress creators first presented by Tarafdar, Ragu-Nathan, and Ragu-Nathan (2007). The chosen research method was survey. This thesis utilized confirmatory factor analysis to test the model for measuring technostress with survey questions. Independent samples T-test was used to test statistical differences between password manager users and non-users, finding out that password manager non-users experience a statistically significantly higher amount of technostress. The objectives of this thesis were met, and research questions were answered. Both research questions, “Do password managers cause technostress?” and “Is

there a difference between in technostress levels between password manager users and non-users?" could be answered affirmatively based on the results of the study. Open survey questions provided additional insight on attitudes towards password managers. It was found that password manager users primarily use them for password memorability, password security, convenience, and easier password management. Non-users reported that their primary reasons to not use password managers are lack of need, distrust, inactivity, and reluctance.

Some of the limitations of this thesis include the fact that the study measures technostress at a very general level and does not go into specifics as of why technostress is being experienced. Furthermore, this thesis does not explore differences in technostress among different groups, such as different age brackets, genders, or the specific causes of technostress.

In conclusion, this study found that password manager users experience less technostress than non-users. This paves the way for further technostress research regarding password managers and can potentially help password manager providers to improve their products to be more appealing for potential users who are still reluctant to use password managers.

REFERENCES

Agarwal, R., & Prasad, J. (1999). Are individual differences germane to the acceptance of new information technologies?. Decision sciences, 30(2), 361-391.

Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. Journal of Applied Psychology, 86(4), 797.

Al-Aameri, A. S. (2000). Job satisfaction and organizational commitment for nurses. *Saudi medical journal*, *21*(6), 531-535.

Arias-Cabarcos, P., Marín, A., Palacios, D., Almenárez, F., & Díaz-Sánchez, D. (2016). Comparing password management software: toward usable and secure enterprise authentication. IT Professional, 18(5), 34-40.

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. MIS quarterly, 831-858.

Beehr, T. (1998). An organizational psychology meta-model of occupational stress. Theories of organizational stress, 6-27.

Benbasat, I., & Barki, H. (2007). Quo vadis TAM?. *Journal of the association for information systems*, *8*(4), 7.

Brod, C. (1982). Managing technostress: optimizing the use of computer technology. Personnel Journal, 61(10), 753-57.

Brod, C. (1984). Technostress: The human cost of the computer revolution. Basic books.

Burke, R. J. (1993). Organizational-level interventions to reduce occupational stressors. Work & Stress, 7(1), 77-87.

Burton-Jones, A., & Hubona, G. S. (2005). Individual differences and usage behavior: revisiting a technology acceptance model assumption. ACM

SIGMIS Database: the DATABASE for Advances in Information Systems, 36(2), 58-77.

Califf, C. B., Sarker, S., & Sarker, S. (2020). The Bright and Dark Sides of Technostress: A Mixed-Methods Study Involving Healthcare IT. *MIS Quarterly*, *44*(2).

Cartwright, S., & Cooper, C. L. (1997). Managing workplace stress (Vol. 1). Sage.

Charness, N., & Boot, W. R. (2009). Aging and information technology use: Potential and barriers. Current directions in psychological science, 18(5), 253-258.

Cheloha, R. S., & Farr, J. L. (1980). Absenteeism, job involvement, and job satisfaction in an organizational setting. Journal of applied Psychology, 65(4), 467.

Chuttur, M. (2009). Overview of the technology acceptance model: Origins, developments and future directions.

Davis, A., & Gibson, L. (1994). Designing employee welfare provision. Personnel review, 23(7), 33-45.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

DeCoster, J. (1998). Overview of factor analysis.

Dragano, N., & Lunau, T. (2020). Technostress at work and mental health: concepts and research results. *Current opinion in psychiatry*, *33*(4), 407-413.

Eddy, E. R., Stone, D. L., & STONE-ROMERO, E. E. (1999). The effects of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives. Personnel Psychology, 52(2), 335-358.

Eslami, J., & Gharakhani, D. (2012). Organizational commitment and job satisfaction. ARPN journal of science and technology, 2(2), 85-91.

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. Human-centric Computing and Information Sciences, 7(1), 1-20.

Fink, A. (2003). How to design survey studies. SAGE Publications, Inc., https://doi.org/10.4135/9781412984447

Galvin, J., Evans, M. S., Nelson, K., Richards, G., Mavritsaki, E., Giovazolias, T., ... & Vallone, F. (2022). Technostress, coping, and anxious and depressive symptomatology in university students during the COVID-19 pandemic. Europe's Journal of Psychology, 18(3), 302.

Gaw, S., & Felten, E. W. (2006, July). Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security* (pp. 44-55).

Gefen, D., & Straub, D. W. (1997). Gender differences in the perception and use of e-mail: An extension to the technology acceptance model. MIS quarterly, 389-400.

Hang, Y., Hussain, G., Amin, A., & Abdullah, M. I. (2022). The moderating effects of technostress inhibitors on techno-stressors and employee's well-being. Frontiers in Psychology, 12, 6386.

Harris, K. J., Harris, R. B., Valle, M., Carlson, J., Carlson, D. S., Zivnuska, S., & Wiley, B. (2022). Technostress and the entitled employee: Impacts on work and family. Information Technology & People, 35(3), 1073-1095.

Heinssen Jr, R. K., Glass, C. R., & Knight, L. A. (1987). Assessing computer anxiety: Development and validation of the computer anxiety rating scale. *Computers in human behavior*, 3(1), 49-59.

Hendrickson, A. R., Massey, P. D., & Cronan, T. P. (1993). On the test-retest reliability of perceived usefulness and perceived ease of use scales. *MIS quarterly*, 227-230.

Holden, R. J., & Karsh, B. T. (2010). The technology acceptance model: its past and its future in health care. Journal of biomedical informatics, 43(1), 159-172.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural equation modeling: a multidisciplinary journal, 6(1), 1-55.

Hudiburg, R. A. (1989). Psychology of computer use: VII. Measuring technostress: Computer-related stress. Psychological Reports, 64(3), 767-772.

Igbaria, M., & Chakrabarti, A. (1990). Computer anxiety and attitudes towards microcomputer use. Behaviour & Information Technology, 9(3), 229-241.

Igbaria, M., & Parasuraman, S. (1989). A path analytic study of individual characteristics, computer anxiety and attitudes toward microcomputers. Journal of Management, 15(3), 373-388.

Ingusci, E., Signore, F., Giancaspro, M. L., Manuti, A., Molino, M., Russo, V., ... & Cortese, C. G. (2021). Workload, techno overload, and behavioral stress during COVID-19 emergency: The role of job crafting in remote workers. Frontiers in psychology, 12, 655148

Ion, I., Reeder, R., & Consolvo, S. (2015). {"... No} one Can Hack My {Mind"}: Comparing Expert and {Non-Expert} Security Practices. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (pp. 327-346).

Jebb, A. T., Ng, V., & Tay, L. (2021). A review of key Likert scale development advances: 1995–2019. Frontiers in psychology, 12, 637547.

Jena, R. K., & Mahanti, P. K. (2014). An empirical study of Technostress among Indian academicians. International Journal of Education and Learning, 3(2), 1-10.

Kahn, R. L., Wolfe, D. M., Quinn, R. P., Snoek, J. D., & Rosenthal, R. A. (1964). Organizational stress: Studies in role conflict and ambiguity.

Kotrlik, J. W. K. J. W., & Higgins, C. C. H. C. C. (2001). Organizational research: Determining appropriate sample size in survey research appropriate sample size in survey research. Information technology, learning, and performance journal, 19(1), 43.

Lazarus, R. S., & Folkman, S. (1984). Stress, appraisal, and coping. Springer publishing company.

Lazarus, R. S., & Opton Jr, E. M. (1966). The study of psychological stress: A summary of theoretical formulations and experimental findings. Anxiety and behavior, 1, 225-262.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & management*, *40*(3), 191-204.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. Communications of the Association for information systems, 12(1), 50.

Locke, E.A. (1976). The nature and causes of job satisfaction.

Luevanos, C., Elizarraras, J., Hirschi, K., & Yeh, J. H. (2017, December). Analysis on the security and use of password managers. In 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT) (pp. 17-24). IEEE.

McGrath, J. E. 1976. Stress and behavior in organizations. M. D. Dunnette, ed. Handbook of Industrial and Organizational Psychology. Rand-McNally, Chicago, 1351–1395.

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). New York: McGraw-Hill.

Oesch, S., Ruoti, S., Simmons, J., & Gautam, A. (2022, April). "It Basically Started Using Me:" An Observational Study of Password Manager Usage. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-23).

Porter, L. W., Steers, R. M., Mowday, R. T., & Boulian, P. V. (1974). Organizational commitment, job satisfaction, and turnover among psychiatric technicians. Journal of applied psychology, 59(5), 603.

Rabinowitz, S., & Hall, D. T. (1977). Organizational research on job involvement. Psychological bulletin, 84(2), 265.

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. Information systems research, 19(4), 417-433.

Rahimi, B., Nadri, H., Afshar, H. L., & Timpka, T. (2018). A systematic review of the technology acceptance model in health informatics. *Applied clinical informatics*, *9*(03), 604-634.

Ray, H., Wolf, F., Kuber, R., & Aviv, A. J. (2021). Why older adults (Don't) use password managers. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 73-90).

Rizzo, J. R., House, R. J., & Lirtzman, S. I. (1970). Role conflict and ambiguity in complex organizations. Administrative science quarterly, 150-163.

Rosen, L. D., & Maguire, P. (1990). Myths and realities of computerphobia: A meta-analysis. Anxiety research, 3(3), 175-191.

Salanova, M., Llorens, S., & Cifre, E. (2013). The dark side of technologies: Technostress among users of information and communication technologies. International journal of psychology, 48(3), 422-436.

Salo, M., & Pirkkalainen, H. (2019). Älylaitteet ja stressi: Aiheuttajat, seuraukset ja hallintakeinot. Lapset, nuoret ja älylaitteet-Taiten tasapainoon.

Shore, L. M., & Wayne, S. J. (1993). Commitment and employee behavior: Comparison of affective commitment and continuance commitment with perceived organizational support. Journal of applied psychology, 78(5), 774.

Smith, M. S., & Salvendy, G. (1991). Work with Computers: Organizational, Management, Stress and Health Aspects. *Journal of the Operational Research Society*, *42*(4), 344. https://doi.org/10.2307/2583388

Sonnentag, S., & Frese, M. (2013). Stress in organizations. John Wiley & Sons, Inc..

Statista (2022). Number of internet and social media users worldwide as of July 2022. https://www.statista.com/statistics/617136/digital-population-worldwide/

Tarafdar, M., Bolman Pullins, E., & Ragu-Nathan, T. S. (2014). Examining impacts of technostress on the professional salesperson's behavioural performance. Journal of Personal Selling & Sales Management, 34(1), 51-69

Tarafdar, M., Pirkkalainen, H., Salo, M., & Makkonen, M. (2020). Taking on the "dark side"––Coping with technostress. IT professional, 22(6), 82-89.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The impact of technostress on role stress and productivity. Journal of management information systems, 24(1), 301-328.'

Tarafdar, M., Tu, Q., & Ragu-Nathan, T. S. (2010). Impact of technostress on end-user satisfaction and performance. Journal of management information systems, 27(3), 303-334.

Tarafdar, M., Tu, Q., Ragu-Nathan, T. S., & Ragu-Nathan, B. S. (2011). Crossing to the dark side: examining creators, outcomes, and inhibitors of technostress. Communications of the ACM, 54(9), 113-120.

Thurik, R., Benzari, A., Fisch, C., Mukerjee, J., & Torrès, O. (2023). Techno-overload and well-being of French small business owners: identifying the flipside of digital technologies. Entrepreneurship & Regional Development, 1-26.

Tondeur, J., Van de Velde, S., Vermeersch, H., & Van Houtte, M. (2016). Gender differences in the ICT profile of university students: A quantitative analysis. DiGeSt. Journal of Diversity and Gender Studies, 3(1), 57-77.

Upadhyaya, P., & Vrinda. (2021). Impact of technostress on academic productivity of university students. Education and Information Technologies, 26, 1647-1664.

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & privacy*, *2*(5), 25-31.

APPENDIX 1 SURVEY STRUCTURE

Technostress and password managers survey

Hello and thank you for participating in the study!

The purpose of this study is to investigate whether the use or thought of using password managers causes technostress and, if so, whether it deters users from using them.

Password manager refers to software that helps users store, create, and manage passwords. They include standalone desktop versions, built-in or add-on extensions for web browsers, as well as smartphone applications.

Technostress refers to the stress that can be caused by the use of information and communication technology.

Every response counts. Responding to the survey will only take a maximum of 5 minutes. The information provided by the respondents will be processed anonymously and cannot be linked to the respondents. Please respond to the study honestly and truthfully. The information provided for research purposes will be treated with absolute confidentiality. Participation in the study is voluntary. By participating in the study, you agree that the provided information will be used for scientific research purposes.

For more information about the study, you can contact Naomi Woods at (*email address*).

Thank you for your time!

Are you currently using a password manager? (a desktop application, browser-integrated or mobile)
- Yes
- No
Rule: Skip next question if answered "Yes".

Have you used a password manager in the past?
- Yes
- No

I would be forced to use more effort than I can handle when using a password manager. (1 = Strongly disagree. 5 = Strongly agree.)

By using a password manager, I would have less time for other things. (1 = Strongly disagree. 5 = Strongly agree.)

Using a password manager would increase my workload. (1 = Strongly disagree. 5 = Strongly agree.)

I feel that using a password manager would cause me to have less time for other important things in my life. (1 = Strongly disagree. 5 = Strongly agree.)

I feel that using a password manager would invade other parts of my life. (1 = Strongly disagree. 5 = Strongly agree.)

I feel that using a password manager would invade other parts of my life. (1 = Strongly disagree. 5 = Strongly agree.)

I feel that I have to sacrifice my vacation and weekend time to use password manager efficiently. (1 = Strongly disagree. 5 = Strongly agree.)

I feel that I do not know enough about password managers to use them effectively. (1 = Strongly disagree. 5 = Strongly agree.)

I do not find enough time to learn to use password managers. (1 = Strongly disagree. 5 = Strongly agree.)

I find password managers too complex for me to use and understand. (1 = Strongly disagree. 5 = Strongly agree.)

I feel that password managers receiving constant updates makes their usage difficult. (1 = Strongly disagree. 5 = Strongly agree.)

I feel that password managers are constantly changing. (1 = Strongly disagree. 5 = Strongly agree.)

I feel that password managers are frequently receiving updates. (1 = Strongly disagree. 5 = Strongly agree.)

Why do you use password managers?
- Open text
Respondent answers this question if answered “Yes” to the first question.

Why do you not use password managers?
- Open text
Respondents answers this question if answered “No” to the first question.

Age
-25 or under
- 26-35
- 36-45
- 46-55
- 56 or older

Gender
- Male
- Female
- Other
- Prefer not to say

Education
- High school education
- Bachelor’s Degree/Undergraduate
- Master’s Degree/Graduate
- Doctorate Degree
- Other

APPENDIX 2 SURVEY EMAIL

Hei!

Teen pro gradu -tutkielmaa salasananhallintaohjelmistoista ja niiden potentiaalista aiheuttaa teknostressiä käyttäjissään. Tutkielman tarkoituksena on selvittää, aiheuttaako salasananhallintaohjelmistojen käyttö teknostressiä, ja jos aiheuttaa, niin pidätteleekö se käyttäjiä käyttämästä niitä? Jokainen vastaus auttaa minua valtavasti. Olisin erittäin kiitollinen, jos osallistuisitte tutkimukseeni.

Salasananhallintaohjelmistolla tarkoitetaan ohjelmistoa, joka auttaa käyttäjiään varastoimaan, luomaan ja hallinnoimaan salasanoja.

Teknostressillä tarkoitetaan stressiä, jota informaatio- ja viestintäteknologian käyttö voi aiheuttaa

Tutkimus toteutetaan kyselytutkimuksena. Kyselyyn vastaaminen kestää enintään 5 minuuttia. Vastaajien tietoja tullaan käsittelemään anonyymisti, eikä vastauksia voida yhdistää vastaajiin. Tutkimuskäyttöön annettuja tietoja tullaan käsittelemään luottamuksellisesti. Tutkimukseen osallistuminen on vapaaehtoista. Osallistumalla tutkimukseen hyväksyt, että antamiasi tietoja käytetään tieteellisen tutkimuksen käyttöön. Vastaathan perjantaihin 16.6. mennessä, jolloin kysely sulkeutuu. Kyselyyn pääset vastaamaan tästä linkistä:
(Linkki kyselyyn)

Vastaan mielelläni myös mahdollisiin kysymyksiin.

Ystävällisin terveisin,
Aleksi Myntti
Jyväskylän yliopisto
(sähköposti)

Hello!

I am writing a master's thesis on password management software and its potential to cause technostress in users. The purpose of the thesis is to investigate whether the use of password management software causes technostress and, if so, whether it deters users from using them. Every response would be tremendously helpful to me. I would be extremely grateful if you could participate in my study.

A password manager is a software that helps users to store, create and organize passwords.

Technostress refers to stress that is caused by the use of information and communication technologies.

The study is conducted as a survey. Answering the survey takes up to 5 minutes. Respondents' information will be processed anonymously, and responses cannot be linked to individual respondents. Information provided for research purposes will be treated confidentially. Participation in the study is voluntary. By participating in the study, you agree that the information you provide will be used for scientific research purposes. Please respond by Friday, June 16th, as that is when the survey will close. You can access the survey through this link: (Link to the survey)

I will gladly respond to any follow-up questions.

Best regards, Aleksi Myntti
The University of Jyväskylä
(email address)