Heidi Haapaniemi

EXPLORING PERCEPTIONS AND COPING BEHAVIORS REGARDING IMPOSED MULTIFACTOR AUTHENTICATION USAGE: A UNIVERSITY CASE STUDY

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2024

ABSTRACT

Haapaniemi, Heidi
Exploring Perceptions and Coping Behaviors Regarding Imposed Multifactor Authentication Usage: A University Case Study
Jyväskylä: University of Jyväskylä, 2024, 96 pp.
Information Systems, Master's Thesis
Supervisor: Woods, Naomi

Data breaches are a growing concern since they can significantly harm people, organizations, and societies. To protect sensitive data against unauthorized access, efficient technological tools alone do not guarantee security – end users should also act in a secure way. Even though information security heavily depends on users, their behavior and especially maladaptive behavior has been understudied. This thesis addressed this gap by studying several perceptions that have been identified to affect users' behavior and coping methods when faced with a threat. Two adaptive coping methods, strong passwords and multifactor authentication, as well as one maladaptive coping method, defensive avoidance, were included in the study. The case study examined whether there were differences in perceptions and intentions to use the studied coping methods between students who had voluntarily activated multifactor authentication for their university user account and students who had not activated it. The data was collected by an online survey sent to a selected group of students at the University of Jyväskylä and analyzed quantitatively. The study found that students who voluntarily activated multifactor authentication did not have any higher perceptions of threat nor more knowledge, but they found their capability to use multifactor authentication (self-efficacy) higher and the effort required to use it (response costs) lower compared to the other group. The intentions to use strong passwords and defensive avoidance were found to be at similar levels in both studied groups. The results indicate that when making changes in the authentication methods used at an organization, it is useful to consider especially the self-efficacy and the response costs from the user's point of view. Overall, through understanding the user better it is possible to support users in the use of authentication methods and thus improve the organization's security, which in turn can help in reducing security breaches, reputational damages, and financial losses. It is, however, evident that more research into coping mechanisms is needed, especially to further clarify the effects of threat appraisal and the role of maladaptive coping behaviors in the context of information security.

Keywords: cyber security, data breach, protection motivation theory, coping behavior, multifactor authentication, passwords

TIIVISTELMÄ

Haapaniemi, Heidi
Pakotettuun monivaiheiseen tunnistautumiseen liittyvät käsitykset ja selviytymiskäyttäytyminen: tapaustutkimus yliopistosta
Jyväskylä: Jyväskylän yliopisto, 2024, 96 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Woods, Naomi

Tietomurrot aiheuttavat yhä enenevissä määrin huolta, sillä ne voivat vahingoittaa merkittävästi ihmisiä, organisaatioita ja yhteiskuntia. Pelkät tehokkaat teknologiset työkalut eivät yksin takaa, että arkaluonteiset tiedot olisivat suojassa luvattomalta käytöltä – myös loppukäyttäjien tulee toimia turvallisella tavalla. Vaikka tietoturva on vahvasti riippuvainen käyttäjistä, ei heidän käyttäytymistään eikä varsinkaan sopeutumatonta käyttäytymistä ole tutkittu tarpeeksi. Tässä pro gradu -tutkielmassa tätä alitutkittua aihetta käsitellään tutkimalla käsityksiä ja selviytymismenetelmiä, joiden on todettu vaikuttavan käyttäjien käyttäytymiseen heidän kohdatessaan uhkia. Tutkimukseen sisällytettiin kaksi adaptiivista selviytymismenetelmää, vahvat salasanat ja monivaiheinen tunnistautuminen, sekä yksi epäadaptiivinen selviytymismenetelmä, suojautuva välttely. Tapaustutkimuksessa selvitettiin, oliko opiskelijoiden, jotka olivat vapaaehtoisesti aktivoineet monivaiheisen tunnistautumisen yliopiston käyttäjätililleen, ja opiskelijoiden, jotka eivät olleet aktivoineet sitä, välillä eroja käsityksissä ja aikomuksissa käyttää tutkittuja selviytymismenetelmiä. Aineisto kerättiin verkkokyselyllä, joka lähetettiin rajatulle joukolle Jyväskylän yliopiston opiskelijoista, ja se analysoitiin kvantitatiivisesti. Tutkimuksessa selvisi, että vapaaehtoisesti monivaiheisen tunnistautumisen aktivoineilla opiskelijoilla ei ollut korkeampaa uhkakuvaa eikä enempää tietoa, mutta he kokivat kykynsä käyttää monivaiheista tunnistautumista (minäpystyvyys) paremmaksi ja sen käyttämiseen vaadittavan vaivan (kustannukset) pienemmäksi verrattuna toiseen ryhmään. Aikomukset käyttää vahvoja salasanoja ja suojautuvaa välttelyä olivat molemmissa tutkituissa ryhmissä samalla tasolla. Tulokset osoittavat, että muutettaessa organisaatiossa käytettäviä tunnistautumismenetelmiä on hyödyllistä ottaa huomioon erityisesti minäpystyvyys ja kustannukset käyttäjän näkökulmasta. Kaiken kaikkiaan, käyttäjiä paremmin ymmärtämällä on mahdollista tarjota heille tukea tunnistautumismenetelmien käytössä ja siten parantaa organisaation turvallisuutta, mikä puolestaan voi auttaa vähentämään tietovuotoja, mainehaittoja ja taloudellisia menetyksiä. On kuitenkin selvää, että selviytymismekanismeja on syytä tutkia lisää erityisesti uhkien arviointitekijöiden vaikutusten ja epäadaptiivisen selviytymiskäyttäytymisen roolin selkiyttämiseksi tietoturvan kontekstissa.

Asiasanat: kyberturvallisuus, tietomurto, suojelumotivaatioteoria, selviytymiskäyttäytyminen, monivaiheinen tunnistautuminen, salasanat

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

In recent years, news about cyber security threats and security breaches has raised concerns about information privacy in Finland. Data breaches concern anyone using digital services, and examples of this are shown in the news: personal information of about 20 000 people was leaked in a breach that concerned two Finnish hotels (Loula, 2022) and dozens of unauthorized bank transfers were made from bank accounts in a Finnish bank (Helpinen, 2022). Another case, the data breach of a Finnish psychotherapy clinic, concerned over 30 000 persons (Hämäläinen, 2021) which makes it one of the biggest criminal cases in Finland by the number of injured parties (Hämäläinen & Rummukainen, 2020). Later on, the highly sensitive data has been used for crimes such as order frauds (Leponen, 2022). The war in Ukraine also brought cyber security concerns to the news headlines (Hallamaa, 2022), and cyberattacks have been performed against several websites of Finnish ministries and government (Paajanen, Keski-Heikkilä, & Halminen, 2022). Cyberattacks are a growing concern in the world since they can significantly harm people, organizations, and societies. Therefore, it is critical to continue developing countermeasures against cyber threats to secure sensitive data.

Unauthorized access is one of the biggest security threats (Velásquez, Caro, & Rodríguez, 2018), which makes authentication a fundamental component of cyber security. Many organizations including the University of Jyväskylä have adopted a multifactor authentication (MFA) scheme instead of continuing using a single-factor authentication method such as the highly prevalent combination of a username and a password. Passwords have not been found secure in a long time (Aloul, Zahidi, & El-Hajj, 2009) despite the many efforts made to make them secure (Sharma, Belwal, Ojha, & Agarwal, 2010). Additionally, passwords are often found difficult to remember and use (Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Vu et al., 2007; Woods & Siponen, 2018, 2019). MFA methods provide secure and user-friendly ways to authenticate (Ometov et al., 2018), which is not possible with passwords that are associated with the tradeoff between security and usability.

Users are often seen as the weakest link in information security and have been understudied in the research literature (Crossler et al., 2013; Datta et al., 2022; Schneier, 2015) despite the fact that information security heavily depends on them (Rhee, Kim, & Ryu, 2009). It is not only enough to develop effective technological tools to enhance information security – end users should also act in a secure way (Herath & Rao, 2009). The combination of both technical and non-technical measures has been found effective in lowering the risk of cyberattacks (Heartfield & Loukas, 2015). Several factors have been identified to affect users' behavior when faced with a threat: threat appraisal (Floyd, Prentice-Dunn, & Rogers, 2000; Rogers, 1975), coping appraisal (Chenoweth, Gattiker, & Corral, 2019; Floyd et al., 2000; Herath & Rao, 2009; Mwagwabi, McGill, & Dixon, 2018; Zhang & McDowell, 2009), knowledge (De Kimpe, Walrave, Verdegem, & Ponnet, 2022; Kovačević, Putnik, & Tošković, 2020; Rochat & Ragot, 2022; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010), trust (De Kimpe et al., 2022) and fear (Johnston, Warkentin, & Siponen, 2015; Mwagwabi et al., 2018; Rogers, 1975; Vance, Eargle, Eggett, Straub, & Ouimet, 2022; Zhang & McDowell, 2009). However, the effect of these factors on users' adaptive and maladaptive coping behavior requires more research. It may be risky to overlook the possibility of maladaptive behavior because some people may end up responding to a threat in a maladaptive, insecure way (Chenoweth et al., 2019) instead of learning to cope with a threat in an adaptive, beneficial way.

This thesis presents an empirical case study that examines students' perceptions and coping behaviors regarding securing their user accounts at the University of Jyväskylä. Two adaptive coping actions are studied: the use or intention to use strong passwords and multifactor authentication. Both authentication methods were available for securing students' user accounts at the University of Jyväskylä at the time of the study. Previous research has additionally pointed out that especially maladaptive coping has been insufficiently researched in the field of information systems (Chenoweth et al., 2019), and maladaptive responses are recommended to be included in studies (De Kimpe et al., 2022). Thus, one maladaptive coping action is studied: defensive avoidance, which in the current study context refers to the intention to avoid thinking about the threat of one's university user account being hacked.

The protection motivation theory (PMT) as one of the most powerful explanatory theories in predicting how an individual will respond when faced with a threat (Anderson & Agarwal, 2010) serves as the basis of this study. Several additional explanatory components have been previously added to the theory (Floyd et al., 2000; Johnston et al., 2015; Ng, Zhang, Thong, & Tam, 2021), and, for example, affective dimensions such as fear (De Kimpe et al., 2022) and internet-related contextual factors such as trust (Chen, Luo, & Li, 2022) have been recommended to be included in research of protection motivation. Therefore, the PMT model used in this study has been extended with the component of fear as part of the threat appraisal and with two antecedents of coping and threat appraisals, trust in internet safety and the perceived knowledge about online risks.

This study focuses on examining if there are differences in online security perceptions, intentions to use strong passwords, and defensive avoidance regarding the threat of students' university user accounts being hacked between students who have voluntarily activated MFA and students who have not activated it. The research questions based on the aforementioned objectives are:

> *RQ1*: Are there differences in online security perceptions between students who have activated multifactor authentication for their university user account and those who have not?
>
> *RQ2*: Are there differences in students' intentions to use strong passwords regarding the threat of their university user account being hacked between those who have activated multifactor authentication and those who have not?
>
> *RQ3*: Are there differences in students' intentions to use defensive avoidance regarding the threat of their university user account being hacked between those who have activated multifactor authentication and those who have not?

The chosen literature covers cyber threats and passwords as well as focuses on the most essential research related to protection motivation and coping behaviors. The literature for the thesis is gathered using search words such as "data breach", "cyber security", "passwords", "multifactor authentication", "adaptive behavior", "maladaptive behavior" and "protection motivation theory". The following search engines were used: IEEE Xplore Digital Library, ACM Digital library, ScienceDirect, ResearchGate, and Google Scholar.

The chapters of this thesis are organized as follows. The second chapter presents the current state of cyber security and the role of end users in protection from cyber threats such as data breaches. In the third chapter, the essential concepts of protection motivation theory and coping behaviors are explained. The fourth chapter covers the most important aspects of the research on passwords and multifactor authentication. The case organization, the University of Jyväskylä, and the authentication schemes used at the university are introduced in the fifth chapter. The remainder of the thesis is organized as follows: chapter 6 describes the research methodology, chapter 7 presents the results of the study, and in chapter 8 the results are discussed. Finally, chapter 9 provides a conclusion of this thesis.

2 CYBER SECURITY AND THE IMPACT OF END USERS

Cyber security threats can cause significant damage, making them an increasing concern in the modern world. The amount of cyberattacks has increased in Finland according to the number of cyber incident notices from Finnish organizations to the Cyber Security Center of Traficom (Traficom, 2022). On the other hand, Woods and Walter (2022) have claimed that globally the frequency of cybercrimes has not significantly increased after the COVID-19 outbreak in 2020. However, people started using more online technology as a result of the COVID-19 epidemic, and for example, the number of online mental health services has greatly expanded (Monteith et al., 2021). Only counting the number of cyberattacks is insufficient; the many consequences and how cyberattacks affect organizations and individuals must also be assessed. For criminals, committing crimes against information technology systems is a profitable business, not just a pastime (Huang, Siegel, & Madnick, 2018), with financial motive being the most important motivator (LLC Verizon, 2022). In general, it is becoming increasingly vital to pay attention to cyber security.

Most research has previously concentrated on firms, leaving consumers' responses to security breaches largely unexplored (Ablon, Heaton, Lavery, & Romanosky, 2016). Cybercrimes such as data breaches can however cause severe consequences for individuals for example in the form of financial losses or identity theft (Woods & Walter, 2022). Additionally, the main weakness in information security is considered to be the users (Crossler et al., 2013; Schneier, 2015), which makes individuals an essential component in cyber security research.

Cyber security threats and their consequences can cause serious damage to both individual users and organizations such as universities. By protecting information systems against security threats, it is possible to reduce the risk of sensitive information leaking outside of the organization to parties that may use the information to gain benefits or cause harm. In this chapter, the main concepts of cyber security are introduced first. Following that, the key findings of numerous studies related to the human factor being the main point of weakness in cyber security are presented. Finally, methods for preventing and responding to data breaches are discussed.

2.1 Cyber Security and Cybercrimes

The numerous definitions available for cyber security often define it in terms of the associated technology and processes, and frequently, its target is protection (CSRC, 2022; International Telecommunication Union, 2008; NICCS, 2022). One example from the literature is Padallan's (2019) definition of cyber security: "the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access" (p. 8). Another example provided by Buczak and Guven (2016) similarly describes it as "the set of technologies and processes designed to protect computers, networks, programs, and data from attack, unauthorized access, change, or destruction" (p. 1153). On the other hand, cyber security can also be viewed as a target state in which the cyber environment can be trusted and its functioning is secured (Sanastokeskus TSK ry, 2018).

The term cyber security is related to the cyber environment, the operating environment that is formed by one or several digital information systems (Sanastokeskus TSK ry, 2018). The cyber environment "includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks" (International Telecommunication Union, 2008). The cyber environment therefore does not only include technology but also the people using it, the data, and the processes related to it.

The cyber environment along with cybercrime has become part of people's everyday lives relatively quickly in recent decades (Holt & Bossler, 2015). Cybercrime is a novel and complex phenomenon with diverse dimensions. It can be described as offenses that are enabled by computer technology and the internet (Holt & Bossler, 2015) or as "any criminal activity that involves a computer, networked device or a network" (Padallan, 2019, p. 6). Researchers typically divide cybercrimes into two categories: cyber-enabled crimes which are criminal activities existing also offline and facilitated using the internet, and cyber-dependent crimes which are criminal activities specifically targeting information technology including hardware, networks, and data (Leukfeldt & Holt, 2022). Cybercrimes are commonly also divided into categories. Woods and Walter (2022) divide them as follows: cyberattacks, malware, ransomware, fraudulent email, online banking fraud, online sales fraud, unauthorized access, denial of service, and identity theft. Threats to information security, like external targeted attacks, are not always intentional crimes committed by attackers: an attack may occur accidentally or due to human mistake (Wheeler, 2011). It is important to distinguish whether for example a data breach is caused by an intentional crime, by an accident, or by human error.

This study focuses on protection against data breaches caused intentionally by an attacker. A data breach is an unauthorized disclosure of information (LLC Verizon, 2022) where unauthorized access concerns data that is sensitive, protected, or confidential, such as financial data, health-related data, and personally identifiable information (Sen & Borle, 2015). For example, in the study by Onaolapo, Mariconti and Stringhini (2016), Gmail accounts were intentionally left to be stolen by criminals and it was found that the criminals tried to find sensitive data from the accounts to gain financial benefits. For example, the criminals may disclose or sell the credentials online (Onaolapo et al., 2016; Thomas et al., 2017). Data breaches can cause compromises in the confidentiality, integrity, and availability of data leading to significant losses for organizations and individuals (Sen & Borle, 2015). Data breaches involving sensitive data can therefore have profound consequences. Data breaches are surprisingly common – the study by Mayer, Zou, Schaub and Aviv (2021) found that 73% of their survey participants' email addresses had been affected by at least one data breach.

The most common attacks to steal passwords are guessing and theft (Holt, 2011), and one way to steal credentials is to trick people into disclosing them via phishing attacks. Phishing involves the use of semantic social engineering attacks such as fraudulent emails and fake websites that deceive users while passing technological security measures (Heartfield & Loukas, 2015; Khonji, Iraqi, & Jones, 2013). Phishing attacks take advantage of human psychology to make people believe the email or website is authentic and secure, making them comfortable to disclose sensitive information like login credentials or open a harmful email attachment (Heartfield & Loukas, 2015).

When recipients of phishing emails feel that the email topic is relevant to them or contains urgency cues that evoke feelings of threat, fear, or an urgent need to act, they are more likely to take the desired action (Vishwanath, Herath, Chen, Wang, & Rao, 2011). The cues are phishing indicators that people can look for when trying to distinguish legitimate emails from phishing emails (Sturman et al., 2023). When attackers emphasize the need to take a recommended action immediately by using wordings emphasizing urgency, people do not take the time and effort to study the email contents and may make mistakes (Vishwanath et al., 2011). It makes no difference if the person is highly educated, experienced, or aware of the risks posed by phishing. Receiving and processing large numbers of emails routinely increases the likelihood of becoming a phishing victim because fast processing limits the time that can be spent thinking about the email's contents (Vishwanath et al., 2011).

Sometimes it is not clear what consequences cybercrimes cause because cybercrimes can have indirect consequences (Woods & Walter, 2022). Cybercrimes that have unclear consequences, for instance, phishing emails and malware, have been found to succeed in victimizing more individuals than cybercrimes that can explicitly cause losses. For instance, phishing can lead to identity theft which can have serious negative effects on the victim's life, and online banking frauds often result in immediate loss of money (Woods & Walter, 2022).

Additionally, cybercrimes can have indirect social and financial impacts on society through the avoidance of using online services, which means that the potential users of a service do not use it and thus do not benefit from it (Riek, Böhme, & Moore, 2016).

2.2 End Users as the Main Point of Weakness

Information security research has been concentrating on the technical side even though the main information security weakness is the individual using the technology (Crossler et al., 2013; Schneier, 2015). Users are typically seen as the weakest link in information security because they frequently make unwise decisions leading to behavior that may expose them to threats (West, Mayhorn, Hardee, & Mendel, 2009). End users are also often not aware of cyber security threats which makes social engineering attacks targeting individuals fairly simple and popular for attackers (Aldawood & Skinner, 2020). Since end users are the weakest link in the chain of information security, it is crucial to consider end-user behavior and minimize any potential human error hazards through creative solutions while developing information systems and processes (West et al., 2009).

The literature handling cyberattacks has been missing the users' perspective while concentrating on serving the interests of technical professionals (Datta et al., 2022). However, for example in Finland's cyber security strategy (Turvallisuuskomitea, 2019), individuals are seen as important actors from the perspective of national cyber security. Authorities, the corporate community, organizations, and citizens are all seen to play a role in Finnish national cyber security. Everyday actions of ordinary people are considered important in enhancing both personal and general cyber security (Turvallisuuskomitea, 2019).

Diverse groups of people have varying tendencies to fall victim to cybercrimes. Women can be slightly more in danger than men, but the difference between men and women may be caused by the differences in the amount of technical knowledge (Sheng et al., 2010). Despite the common misconception that younger adults aged less than 25 years old are more accustomed to interacting with the internet world, they are in fact more at risk of becoming victims of cybercrimes than older age groups (Debb, Schaffer, & Colson, 2020). For example, younger people fall victim to email phishing attacks more probably than older people (Sheng et al., 2010), and password sharing is more common among younger people than among older individuals (Whitty, Doodson, Creese, & Hodges, 2015).

Suggested reasons behind younger people's higher victimization rates include young people having less education and less experience using the internet, and that they tend to avoid risks less often (Sheng et al., 2010). Other reasons include having been involved in fewer information security trainings (Sheng et al., 2010) and having less awareness of cyber security best practices such as following the recommended policies and knowing how to react to alerts or messages from software (Debb et al., 2020). Another explanation is that young people use more online services (Eurostat, 2023) and a wider range of technologies (Olson, O'Brien, Rogers, & Charness, 2011), and this creates more opportunities for cybercrime to occur. Using information technology more may lead to behaving less securely and frequent information technology use does not mean that one has the required cyber security knowledge and means to be able to protect oneself against cyber threats (Kovačević et al., 2020). The most active users of social networks are often the easiest targets because their large number of friends or connections makes it more difficult for them to quickly identify whether the acquaintance is really a friend or not, leading to, for example, clicking the links that the attackers send (Vishwanath, 2015). Different age groups also experience cyber security differently; whereas children engage more with positive and social aspects of cyber security, adults emphasize malicious activities, anxiety, and protective aspects (Jones, Collins, Levordashka, Muir, & Joinson, 2019).

Security experts and non-experts have been found to have quite similar perceptions of online risks related to activities such as online service use, location sharing, and opening emails from unknown senders (Creese, Hodges, Jamison-Powell, & Whitty, 2013). In the study by Creese et al. (2013), the only difference found was that experts found not updating applications more severe than non-experts did. In another study, users from a computer science school were found to have more than 1,8 times stronger passwords than business school users (Mazurek et al., 2013) which suggests that differences in password strength may be related to knowledge. Experiencing a security compromise did not differentiate how non-experts assessed online risks in the study conducted by Creese et al. (2013). However, in another study, experiencing cybercrime was found to increase the perceived cybercrime risk which indirectly raised intentions to avoid utilizing online banking and shopping services (Riek et al., 2016).

Other factors such as mental health, a person's thinking, and culture can also have an influence on the security behavior of the individual. It is not easy to identify the most vulnerable users (Albladi & Weir, 2018). People with mental illnesses may be more likely to become victims of cybercrimes because they may not be aware of risks online, how to prevent falling victim to cybercrimes, and what to do after falling victim to a cybercrime (Monteith et al., 2021). Over-optimism has been found to be one reason for end users being the weakest link in information security: when people are overly optimistic about their safety online, they do not find it necessary to perform online safety measures (De Kimpe et al., 2022). In the study by Whitty et al. (2015), it was discovered that monitoring and controlling one's own behavior more increased the chance of sharing passwords. Another password study showed that there were a lot of similarities between passwords created by users from different language communities (Bonneau, 2012). Culture, however, has been found to have a significant role in online security behavior – a study between users from the United States and China revealed that national and individual differences as well as the culture that the individual had adopted influenced the individual's threat perceptions and behaviors in regards to, for example, seeking for help and using avoidance as a coping mechanism (Chen & Zahedi, 2016). In their findings, Chen and Zahedi (2016) suggest that by researching how people with certain characteristics or from a certain culture tend to behave, it is possible to develop strategies that best support individuals to adopt safe coping behaviors.

2.3 Protection Against Cyber Threats

Several studies have shown that a combination of technical and non-technical measures is effective in lowering the risk of cyberattacks (Heartfield & Loukas, 2015). Several solutions for preventing and responding to cyber threats have been developed, including the use of antivirus software, firewalls, and other security measures, as well as user education and training (Cain, Edwards, & Still, 2018). Technical measures include using new technologies such as machine learning and data mining that can be used to enhance intrusion detection and improve system security (Buczak & Guven, 2016). For example, account compromission attacks can be spotted faster by models that detect unusual email search behavior (Onaolapo et al., 2016). While technical measures, such as antivirus software and firewalls, are important for protecting against specific types of cyberattacks, they are not sufficient on their own, and non-technical measures like user education and training are also needed.

It is important to keep in mind that information systems depend on interactions between people, technology, and the environment (West et al., 2009). Online social deception attacks are examples of attacks specifically targeting human beings, combining knowledge and resources from a variety of disciplines, including engineering, psychology, linguistics, and sociology (Guo et al., 2021). From the technological perspective, cyberattack defense can be strengthened by increasing the understanding of cyberattack business because similar types of technological innovations can be used both for cyberattacking and defending against cyberattacks (Huang et al., 2018). Bringing together the expertise of many professional groups is thus essential to developing efficient solutions to defend against cyber threats (Guo et al., 2021).

Information security heavily depends on end users and how they behave in terms of information security (Rhee et al., 2009). A human factor was present in most breaches in Verizon's data of incidents between November 2020 to October 2021 (LLC Verizon, 2022). In one study, the participants who had fallen victim to at least one data breach involving their email address believed that they were affected by a data breach because of their own behavior (Mayer et al., 2021). By putting more attention into understanding the individuals it is possible to see them as security allies instead of mere security risks (Crossler et al., 2013).

The key element in promoting cyber security awareness has been considered to be knowledge. Acquiring the required knowledge helps in being more aware of and protecting oneself from cyber threats (Kovačević et al., 2020) and in understanding the importance of, for example, secure passwords (Adams & Sasse, 1999; Grawemeyer & Johnson, 2011). However, awareness of risks in itself has been researched not to be linked to the risks of phishing (Vishwanath et al., 2011) and people have been found not to seek out to gain more knowledge about cyber security or how to act more securely online even though they believed that their data was not safe (Kovačević et al., 2020). Even non-expert users have been found to be sufficiently knowledgeable about most of the fundamental online security practices (Creese et al., 2013) which suggests that the majority of users already have a basic understanding of cyber security. Also, even though people seem to often know how to make passwords stronger, they do not do so (Ur et al., 2016).

Different types of knowledge may have varying effects on users' information security behavior. By increasing the knowledge meaningful to the end users it is possible to increase users' understanding of cyberattacks and help users protect themselves from being exposed to certain risks (Datta et al., 2022). Training against an attack type, for example cue-based training against phishing emails, has been proven to help individuals protect themselves from threats (Sturman et al., 2023). In a study by Sheng et al. (2010), the participants were even 40% less likely to give information on phishing websites after receiving specific information security training. One drawback noticed in the study was that people were not only less likely to click on phishing links, but they were also less likely to click on genuine, non-harmful links. Additionally, despite receiving training, 28% of the study participants fell for the conducted phishing tests, showing that information security training is not a perfect solution for helping people protect themselves from information security hazards (Sheng et al., 2010).

To promote information security in organizations, it is not enough to develop effective technological tools but also information security policies are needed to ensure the end users act in a secure way (Herath & Rao, 2009). It has been found possible to motivate employees to comply with the information security policies by emphasizing the need for protection or by the opportunity to avoid pain caused by informal sanctions (Johnston et al., 2015). However, every person is unique, and some are more motivated by protection and some by the opportunity to avoid pain (Johnston et al., 2015). The employees' understanding of the severity of information security threats also affects their concern over security breaches (Herath & Rao, 2009). This, however, does not mean that the employees would comply better with the information security policies: if complying with the policies is considered troublesome, people will not be willing to comply with them. By informing individuals how their efforts can have a positive impact on cyber security, they can be motivated to take action (Herath & Rao, 2009).

To summarize, cybercrimes such as unauthorized access are a major threat that can cause significant harm to individuals, organizations, and societies. While there are various strategies for preventing and responding to these threats, more research is needed to better understand and address this complex and evolving issue. Since most breaches involve a human factor, technical measures alone are not enough to protect against today’s cyber threats. Multiple studies have shown that combining technical measures, such as antivirus software and firewalls, and non-technical measures, such as user education and training, is necessary to effectively mitigate the risk of cyberattacks. In the next chapter, protection motivation and users’ coping strategies are discussed to gain further understanding of individuals and their information security behavior.

3 PROTECTION MOTIVATION AND COPING BEHAVIOR

Protection motivation theory (PMT) is one of the most powerful explanatory theories in predicting how an individual will respond when faced with a threat (Anderson & Agarwal, 2010). In this study, PMT is used as the main theoretical foundation for gaining understanding of individuals' online security behavior in the presence of cyber threats and ways to mitigate these threats. In this chapter, the basic ideas of PMT and related concepts such as fear appeals are introduced first. Then, threat and coping appraisals along with the related coping behavior are presented. Finally, the relationships between PMT and two additional concepts, perceived knowledge, and internet trust, are discussed.

3.1 Protection Motivation Theory

PMT was first proposed by Rogers (1975) in 1975 to increase knowledge about the impact of fear appeals on human behavior, and since then it has been widely used to understand how people make decisions about protecting themselves from perceived threats. Since PMT was first formulated, it has also been refined, and additional explanatory components have been added to it (Floyd et al., 2000; Johnston et al., 2015; Ng et al., 2021), for example self-efficacy (Maddux & Rogers, 1983). The theory has been frequently employed in the area of health behaviors including exercise, diet, smoking, and sun protection (Milne, Sheeran, & Orbell, 2000), but it has also been applied in the context of adopting safety behaviors such as wearing helmets while biking or driving safely (Floyd et al., 2000) as well as responding to cyber security threats (Vance, Siponen, & Pahnila, 2012).

According to PMT, individuals go through a cognitive appraisal process in order to respond to a perceived threat initiated by a fear appeal (Maddux & Rogers, 1983). People protect themselves based on two main factors: threat appraisal and coping appraisal (FIGURE 1). Threat and coping appraisals motivate a person to process the concept of protection motivation and to initiate behavioral intention by making the decision to start, continue, or stop implementing a coping strategy (Floyd et al., 2000). Adaptive behavior can be promoted by higher coping appraisal and maladaptive behavior by higher threat appraisal (Floyd et al., 2000). Both types of behavior are responses to a given situation and are motivated by appraisals. These appraisals and coping processes will be described in detail later.

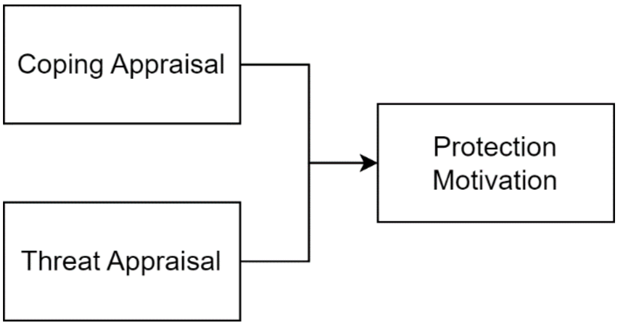

FIGURE 1 Protection Motivation Theory

PMT has been considered applicable to any threat threatening an individual if there is a protective measure that the individual can take to protect themself from the threat (Floyd et al., 2000). However, PMT and other behavioral theories involving fear appeals have often been defined incorrectly in information security research (Johnston et al., 2015). For example, in an organizational setting, the fear sanction models have not been able to adequately explain why employees do not comply with the organization's information security policies and instead circumvent them (Siponen & Vance, 2010).

3.2 Fear Appeals

Fear appeals have been researched separately and as part of the PMT's threat appraisal process. Fear appeals are persuasive messages that use a sense of fear connected with a threat to encourage users to take the advised actions (Johnston & Warkentin, 2010). Fear appeals are often used to motivate and guide users to protect themselves from information security threats (Johnston et al., 2015; Vance et al., 2022). Fear of threat has been found to influence use intentions (Mwagwabi et al., 2018; Zhang & McDowell, 2009), although fear as an emotional state does not directly motivate change; rather, it influences cognitive processes that influence behavioral intention for protection motivation (Rogers, 1975).

Researchers have not been able to verify the effectiveness of fear appeals in the field of information security and for example its effect on compliance with information security policies and processes (Johnston et al., 2015). Johnston and Warkentin (2010) discuss that even though end-user behavioral intentions to act securely as recommended are impacted by fear appeals, all end users are not influenced in the same way. Commonly described cognitive processes of PMT are severity, susceptibility or vulnerability, efficacy of the advised action, and individual's capability to complete the advised action, which all impact how well fear appeals work (Johnston & Warkentin, 2010).

3.3 Threat Appraisal and Maladaptive Coping Behavior

Fear appeals are closely linked to threat appraisal (Maddux & Rogers, 1983). Threat appraisal refers to people's assessment of a threat: how people perceive a threat by evaluating the severity of it and the likelihood of it occurring (Maddux & Rogers, 1983). Threat appraisal is the first step to trigger the motivation to protect oneself because processing a threat comes first before considering how to cope with it (Floyd et al., 2000).

Threat appraisal involves evaluating the severity and the vulnerability, or susceptibility, of a threat (Floyd et al., 2000; Rogers, 1975). The aspect of perceived severity refers to the perception of how serious the threat is, including the evaluation of the potential harm that can come from it. Perceived vulnerability is related to the likelihood of being affected or harmed by the threat. When defining the level of threat appraisal, two types of rewards may also be evaluated: intrinsic and extrinsic rewards (Floyd et al., 2000). Intrinsic rewards come from within the person and give physical or psychological pleasure like enjoying mental stimulation and extrinsic rewards come from external sources like peers approving one's behavior. FIGURE 2 describes the composition of threat appraisal.

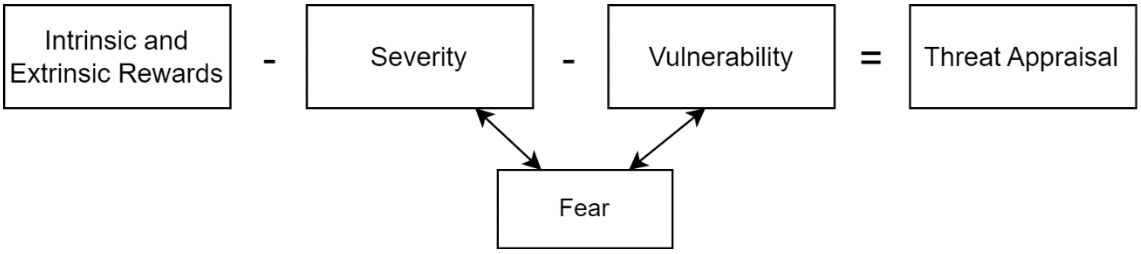

FIGURE 2 Threat Appraisal

De Kimpe et al. (2022) found that greater perceived severity and vulnerability of a cybercrime risk made people more likely to take countermeasures against cybercrime. For example, higher perceived email communication risk has been found to increase the feeling of usefulness of an email authentication service, which verifies the sender domain of an email, and the users' intention to adopt it (Herath et al., 2014). Additionally, in the context of malware threats, it has been researched that higher perceived severity is associated with internet users being more motivated to protective behavior (Dang-Pham & Pittayachawan, 2015). On the other hand, threat appraisals of perceived severity and vulnerability have not always been found to have a direct effect on use intentions (Mwagwabi et al., 2018).

Haag, Siponen and Liu (2021) underline that measuring individuals' level of concern about information security threats is useful because users cannot be assumed to feel concerned about all information security threats: for some the threats may feel more concerning than for others. Similarly, De Kimpe et al. (2022) discovered that even when people perceive online risks as serious, they may believe they are so well-informed about them that they are less exposed to cybercrime and do not need to spend the effort to engage in activities that improve online security. Therefore, the authors emphasize how important it is to educate individuals about the fact that believing not to be vulnerable to online threats does not lessen the severity or likelihood of falling victim to cybercrime (De Kimpe et al., 2022).

Even if a person feels threatened by a threat, they do not always act adaptively. A high perception of threat appraisal has been linked to maladaptive behavior (Floyd et al., 2000). Maladaptive coping mechanisms are ways of responding to a threat in a way that is often counterproductive (Chenoweth et al., 2019). The risk of maladaptive coping behavior has been found to be high if the person has a high threat appraisal combined with a low coping appraisal (Chenoweth et al., 2019).

Over 20 forms of maladaptive coping have been identified in the behavioral literature (McCrae, 1984). Examples of these forms are avoidance, social comparison, hostile reaction, and fatalism. For example, people may not be willing to act adaptively by using multifactor authentication to protect their online service user account if they think that other people are not using it (social comparison), or if they instead prefer to disregard that their user account could be vulnerable to a data breach (defensive avoidance) (Xie, Siponen, Moody, & Zheng, 2022), or if they prefer avoiding utilizing online services (behavioral avoidance) (Riek et al., 2016). Consequently, maladaptive behavior can cause harm rather than improve the situation, leaving the individual straining to deal with the threat or, in the worst-case scenario, suffering from the consequences of falling victim to cybercrime.

Maladaptive coping has been insufficiently researched in the field of information systems (Chenoweth et al., 2019). When designing interventions, trainings, or information security campaigns, it can be risky to overlook the possibility of maladaptive behavior because, as shown in studies, some people may end up responding to threats in insecure ways (Chenoweth et al., 2019) instead of learning to cope with a threat in beneficial ways.

3.4 Coping Appraisal and Adaptive Coping Behavior

Coping appraisal means how people evaluate their ability to deal with a threat (Maddux & Rogers, 1983). It is related to assessing the potential coping strategies and is essential for making the ultimate decision about whether to act or not (Maddux & Rogers, 1983). According to research, coping appraisal constructs are more important in terms of enhancing information security compliance than threat appraisal constructs (Mwagwabi et al., 2018).

Coping appraisal is essentially linked with the evaluation of adaptive behavior which consists of useful ways to constructively protect oneself from a threat (Chenoweth et al., 2019). Examples of adaptive behavior are using antispyware software (Johnston & Warkentin, 2010) and using strong passwords to protect a user account (Grimes & Marquardson, 2019). Another example of adaptive behavior is to deal with phishing threats by using an email authentication service that verifies the email sender domain (Herath et al., 2014). In a study that researched the adoption of an email authentication service, the participants who were confident in their skills and believed they could deal with email threats themselves were less motivated to adopt the service. On the other hand, participants with a high level of two coping-related factors, perceived usefulness and perceived ease of use, had an increased motivation to adopt the service (Herath et al., 2014).

As shown in FIGURE 3, coping appraisal is often described to consist of three constructs: response efficacy, self-efficacy, and response costs (Floyd et al., 2000). The construct of response efficacy is the belief that a coping strategy will be effective in reducing the threat (Maddux & Rogers, 1983). When response efficacy is high, the person believes that the adaptive response will be effective for protection (Floyd et al., 2000). The construct of self-efficacy is a person's belief that they are capable of performing the adaptive actions successfully (Floyd et al., 2000; Maddux & Rogers, 1983). When self-efficacy is high, a person's intention to protect themself from cybercrime has been found to increase (De Kimpe et al., 2022). The last construct, response costs, are the costs effective when a person takes adaptive coping actions, for example the effort needed to act or the loss of time or money (Floyd et al., 2000). Adaptive behavior has been found to be promoted by high response efficacy (Floyd et al., 2000; Herath & Rao, 2009; Mwagwabi et al., 2018; Zhang & McDowell, 2009) and high self-efficacy (Floyd et al., 2000; Mwagwabi et al., 2018), and discouraged by high response costs (Floyd et al., 2000; Zhang & McDowell, 2009).

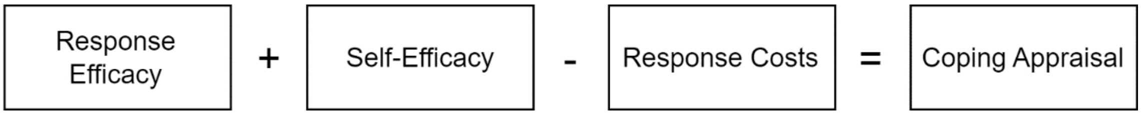

FIGURE 3 Coping Appraisal

3.5 Perceived Knowledge and Trust

In several studies, PMT has been complemented by the concepts of perceived knowledge, and trust (FIGURE 4). For example, in the study by De Kimpe et al. (2022), the goal of examining perceived knowledge and internet trust was to help understand how optimistic individuals are about internet safety and how it affects their mental processes while deciding which actions to take to protect themselves against threats.

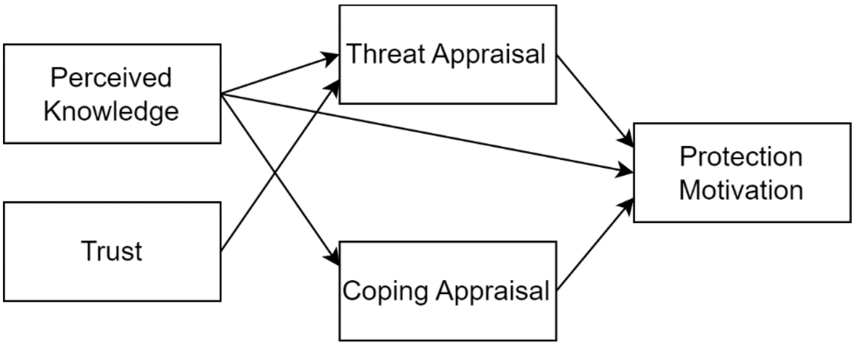

FIGURE 4 Protection Motivation Theory Complemented by Perceived Knowledge and Trust

Up to now, cybersecurity and PMT research have paid little interest in perceived knowledge (De Kimpe et al., 2022). Higher perceived knowledge has been found to constrain reactions to fear appeals (Nabi, Roskos-Ewoldsen, & Dillman Carpentier, 2008). However, the relationship between knowledge and behavior is not simple (Kemp, 2023), and knowledge about countermeasures against threats does not protect the person from victimization if the person is not capable of noticing and assessing threats (Hanus & Wu, 2016).

In the context of cybersecurity, perceived knowledge refers to an individual's thinking of whether they have the needed amount of information about threats located online and how to protect themselves from these threats (De Kimpe et al., 2022). There have been varying results on how perceived knowledge and behavioral intention relate depending on the type of knowledge. In the study by De Kimpe et al. (2022), perceived knowledge was found to have a direct negative correlation with protection motivation: the more the individual thought they knew about cyber security threats and how to protect oneself from them, the less motivated they seemed to be to take protective measures. Perceived knowledge has also been examined by for example Rochat and Ragot (2022) who researched the relationship between perceived knowledge, attitude, and adoption intention of Green IT. They found out that in the context of Green IT if a person has a high level of perceived knowledge of Green IT, they have a more positive attitude and higher adoption intention of Green IT (Rochat & Ragot, 2022). Since there have been inconsistent research results on the effect of knowledge, increasing the level of knowledge can be positively or negatively associated with behavioral intention depending on the type of knowledge and the context.

Trust is a complex concept including, for example, the relationship between different parties and being vulnerable to other's actions that can potentially be malicious (Wang & Emurian, 2005). For example, in the context of internet shopping, consumers need to trust the merchant to deliver their order (Lee & Turban, 2001). However, consumers also need to trust the internet when they use it as a medium of online shopping (Lee & Turban, 2001). Internet trust describes the perception of safety related to online activities: how strongly the individual believes that the internet is safe (De Kimpe et al., 2022). If a person trusts that the internet is secure, they will not consider the threats it poses to be serious and will not perceive themselves as being at risk (De Kimpe et al., 2022). Likewise, Pavlou (2003) found that trust reduces the level of perceived risk. De Kimpe et al. (2022) found that internet trust correlated with the perceived threat severity and perceived vulnerability, and, similarly, Chen et al. (2022) found it to be negatively associated with fear and perceived security threat. However, it is not clear if there is a relationship between internet trust and coping appraisal. They have been found not to be associated (De Kimpe et al., 2022), but in contrast, trust has also been found to be associated with perceived coping efficacy (Chen et al., 2022). Additionally, it is not clear if there exists a relationship between trust and protection motivation. De Kimpe et al. (2022) found them not to be linked, but, on the other hand, Chen et al. (2022) found trust to influence adaptive coping behavior but not maladaptive coping behavior such as avoidance.

To summarize, PMT is a widely accepted theoretical framework that helps to understand how individuals respond to perceived threats. PMT has been researched closely with fear appeals that use the fear of threat to motivate users to take protective measures. The theory has been refined multiple times since it was first formulated in 1975, and additional constructs such as perceived knowledge and trust have been added to it. The theory presents threat appraisal and coping appraisal as processes that influence the decisions to take protective actions to protect oneself from threats. A high level of threat appraisal is linked to maladaptive coping behavior and a high level of coping appraisal to adaptive coping behavior. Examining additional constructs, the perceived knowledge of internet risks and internet trust, helps to understand further individuals' protective behavior. The next chapter will introduce two adaptive coping behavior methods, strong passwords and multifactor authentication, which can help in protecting user accounts against unauthorized access.

4 FROM PASSWORDS TO MULTIFACTOR AUTHENTICATION SCHEMES

Unauthorized access by representing oneself as an authorized user despite not being one can be seen as one of the biggest security threats for technological devices (Velásquez et al., 2018), making authentication a fundamental component of cyber security. The goal of authentication is to verify identities (Peisert, Talbot, & Kroeger, 2013). Authentication is the process of proofing a user's identity before granting them access to data in an information system (Banyal, Jain, & Jain, 2013). Additionally, if the access is continuous, the authentication should be continuous rather than a one-time check (Peisert et al., 2013). Authentication should be made easy for users to use but difficult to bypass by unauthorized users (Peisert et al., 2013).

Passwords as an authentication method have not been found secure in a long time (Aloul et al., 2009) despite the many efforts made to make passwords secure (Sharma et al., 2010). Passwords are used in such large numbers that it has become a significant and profitable criminal business to share and sell stolen credentials on the dark web (Thomas et al., 2017). Thus, improving authentication systems is crucial to keep information systems secure. Multifactor authentication (MFA) methods require the user to authenticate using multiple methods, and thus there are several layers of authentication protecting a user account (O'Gorman, Bagga, & Bentley, 2005). Even if one method is compromised, the other method(s) will maintain the security of the authentication (O'Gorman et al., 2005). After the introduction of MFA schemes, there are now better opportunities for providing secure and user-friendly authentication (Ometov et al., 2018).

As individuals have a constantly growing number of online accounts and the threats posed by cyber-attacks are growing in the modern world, it is important to enhance authentication security. In this chapter, the security and usability of the currently widely used password authentication are discussed first, followed by a discussion of ways to enhance password security and usability. Then, multifactor authentication methods as more secure ways to authenticate are described.

4.1 Password Security and Usability

The most used authentication method worldwide continues to be passwords (Al Kabir & Elmedany, 2022; Bonneau, Herley, Van Oorschot, & Stajano, 2012; Gaw & Felten, 2006; Holt, 2011; Vu et al., 2007; Zimmermann & Gerber, 2020), and the use of passwords has been increasing with the number of accounts increasing (Bang, Lee, Bae, & Ahn, 2012; Gaw & Felten, 2006). Since the combination of user ID and password is cost-efficient (Conklin, Dietrich, & Walz, 2004), easy to use (Ezugwu et al., 2023), and easy to implement, it is not expected to be easily replaced by another authentication method (Holt, 2011). Passwords are criticized for being insecure (Furnell, 2022) and vulnerable to attacks (Sharma et al., 2010), and the individual user is often seen as the weakest link in the security chain of securing information assets (Crossler et al., 2013; Schneier, 2015) as users tend to use weak passwords (Bonneau, 2012; Vu et al., 2007). Many computer systems are only as secure as their weakest password (Schneier, 2015), and consequently, weak passwords can endanger the entire system or even another system that is integrated with it (Conklin et al., 2004).

In a study by Holt (2011), it was identified that the most important factor of safe passwords is length, and the second most important factor is complexity. Shen, Yu, Xu, Yang and Guan (2016) discovered that the average length of a password is however only between 8 and 10 characters. Often the average password strength is found to be considerably weak (Bonneau, 2012; Vu et al., 2007). A notable number of users have been found to use the most common passwords or use the login name also as a password (Shen et al., 2016).

Users may not realize what the predictability of their password is and misconceptions about password security are common (Ur et al., 2016). There is an elevated risk that the person's other accounts can be compromised if their passwords or personal data have been exposed in the past or are known to the attacker (Wang, Zhang, Wang, Yan, & Huang, 2016). Criminals most commonly acquire passwords via guessing or theft (Holt, 2011). If one sister password and pieces of personally identifiable information from the victim are known, it is possible to guess the victim's other password at a high success rate (Wang et al., 2016). Most participants in one study thought that withstanding less than 50 000 password guesses is sufficient (Ur et al., 2016) even though passwords should withstand even 10^{14} guesses to be considered secure (Florêncio, Herley, & Van Oorschot, 2014). Attackers are often seen as humans, and many do not recognize the possibility that an automated tool could crack their password with the help of a large dictionary and a large number of tries (Gaw & Felten, 2006). The fact that an individual's perceived security and perceived memorability of a password may not match the actual password security may partially explain the use of poor passwords (Ur et al., 2016). If people do not understand how their passwords can be attacked, they may not feel motivated to invest in making secure passwords (Ur et al., 2016).

Additionally, passwords are still seen as the only part of credentials that should be kept secret even though usernames can be thought of as the first line of defense for accounts (Fandakly & Caporusso, 2020). The same username is frequently used in numerous services (Fandakly & Caporusso, 2020), and often even the same username and password combination is used across many services (Bang et al., 2012). Contrary to passwords, which are frequently configured to expire after a particular period of time, many services do not even permit username changes (Fandakly & Caporusso, 2020) increasing the importance of using strong passwords.

Having strong security policies and mechanisms does not guarantee that a system is secure because creating a secure system requires taking into account end-user behavior and usability (Adams & Sasse, 1999). Textual passwords generated by the user have to deal with the problem of balancing between security and usability (Guo, Zhang, & Guo, 2019). Password entry errors are more common with stronger passwords (Mazurek et al., 2013). Password policies and requirements are used to ensure every password is sufficiently strong, but users may follow them in an easy and insecure manner producing weak passwords (Guo et al., 2019; Vu et al., 2007). Therefore, the challenge is to balance the security and the usability of passwords (Guo et al., 2019).

Already in an early password study by Adams and Sasse (1999), using and changing passwords has been connected to remembering passwords. Several later studies also focus on memorability when discussing password use (Barron, So, & Nikiforakis, 2021; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Vu et al., 2007; Woods & Siponen, 2018, 2019). Password security can be strengthened by proactive means such as demanding the password to meet certain requirements, but the requirements alone do not always lead to stronger passwords (Vu et al., 2007). Password restrictions with the intention to enhance password security may lead to the creation of less memorable passwords that the person may even write down to remember them (Adams & Sasse, 1999).

It is problematic if individuals disregard complex password requirements and try to circumvent them (Siponen, Puhakainen, & Vance, 2020). Users may comply with security rules but use insecure coping mechanisms such as writing passwords down or using common or slightly varying elements in several passwords (Adams & Sasse, 1999; Stobert & Biddle, 2018). These mechanisms compromise password security. According to Stobert and Biddle (2014), users can have complex coping strategies and more effort is used to develop a strong password if the account is found more important.

Numerous studies have explored the password coping strategies that people use. One of the most used coping strategies is password reuse (Adams & Sasse, 1999; Bang et al., 2012; Florêncio & Herley, 2007; Gaw & Felten, 2006; Stobert & Biddle, 2018). In the study by Florêncio and Herley (2007), the average participant had 6,5 passwords that were each used for 3,9 accounts. A study by Gaw and Felten (2006) reveals that when the number of online accounts owned by the user increases, the user does not start creating more passwords but reuses them. Thanks to the reuse, users found managing passwords easier

(Gaw & Felten, 2006). Reused passwords are remembered better than unique ones, and passwords that are never changed are remembered better than ones that have been changed (Grawemeyer & Johnson, 2011). Stobert and Biddle (2018) use the term "password life cycle" to describe the phenomenon where from the moment the password is created, it may be used for a long time for many accounts and modified several times before it is removed from use. Complex coping strategies can thus lead to passwords being developed and then reused and adapted numerous times (Stobert & Biddle, 2018).

Password reuse causes issues that users may not consider: a study on leaked datasets of usernames and passwords estimated that 7-25% of the leaked passwords matched the victim's Google account (Thomas et al., 2017). Another study found that there were similarities between university passwords and passwords leaked from low-value accounts (Mazurek et al., 2013). The consequences of having credentials stolen are more severe if the attacker is able to steal data from several services with the same credentials. For example, Google account credentials can be used to sign in to several applications and services (Google, n.d.). This kind of social login authentication is convenient since it simplifies logging in to services (Parmar, Sanghvi, Patel, & Pandya, 2022) but it is risky in the situation where the account credentials are leaked.

Overall, user's capabilities, motivation, and convenience have been linked to password use. Performance in remembering passwords is not related to memory performance but instead, it has been found to correlate with how well an individual thinks they can remember passwords and how motivated they are to do so, individual's knowledge about how to make memorable passwords and how manageable the individual finds remembering passwords (Woods & Siponen, 2018). There is evidence that users tend to prefer easy-to-type passwords over ones that are more difficult to type. For example, when asked to use special characters in the password, people tend to use the ones that are easy to type (Shen et al., 2016). In addition, the used device affects the password choice at password creation: for example, on mobile devices the users tend to use weaker passwords due to the increased effort required to enter a password (von Zezschwitz, De Luca, & Hussmann, 2014).

4.2 Enhancing Password Security and Usability

Password security can be enhanced, for example, by reminding users to change default passwords, developing technologies that help choose strong passwords, setting password expiration times, preventing password reuse, providing ways to reset passwords, and monitoring the number of unsuccessful login attempts (Holt, 2011). Enhancing user awareness of secure passwords and threats can further help protect passwords from attacks (Holt, 2011). Also, suggestions for better password creation techniques have been made. Mnemonic password creation techniques that aid memory can be based on expressions or sentences

(Barton & Barton, 1984), images (Nelson & Vu, 2010), shapes (Song, Wang, Yun, & Han, 2019), or keyboard figures (Guo et al., 2019).

Even though encouraging and guiding users to create strong passwords is more effective in enhancing password security than strict password rules (Yıldırım & Mackie, 2019), password creation support is rarely given to the user on websites (Furnell, 2007). The technology systems often do not support the culture of strong passwords and instead, they enable poor practices in password management (Gaw & Felten, 2006). For example, making resetting passwords quick and easy can encourage users to comply with password policies since it is easier to use secure passwords if recovering from a situation of a forgotten password is easy (Holt, 2011).

Guiding users can help in the creation of stronger passwords and thus improve information security (Furnell, Esmael, Yang, & Li, 2018). Several research papers suggest that it is possible to help the user in the password creation phase and make using passwords more user-friendly and secure. For example, providing richer information such as messages showing the time required to crack the selected password or the relative ranking of the password against other passwords can motivate the user to choose a stronger password (Furnell et al., 2018). Using just graphical feedback to help users choose stronger passwords enhances the password strength only by a small amount (Bonneau, 2012), whereas a password meter with detailed feedback can make users create equally memorable but stronger passwords than a plain password meter with no other feedback than a bar showing the password strength (Ur et al., 2017). Furthermore, users have been found to create stronger passwords with a password meter that additionally includes peer feedback (Dupuis & Khan, 2018).

The participants of the early password study by Adams and Sasse (1999) lacked sufficient knowledge of the components of safe passwords and how passwords are cracked, whereas nowadays a lot of information about passwords is available online. However, both insufficient and erroneous knowledge can lead to the use of insecure password strategies such as password reuse, sharing, and writing down (Grawemeyer & Johnson, 2011). Users with insecure password behavior could be guided to adopt secure password strategies (Grawemeyer & Johnson, 2011), but most websites still do not provide appropriate guidance to users and may even allow the use of very insecure passwords such as "password" (Furnell, 2022). The lack of progress in authentication systems and user support in the last decade is concerning, but in the future, it is expected that organizations will move from simple password authentication to authentication with multiple methods making authentication more secure (Furnell, 2022).

4.3 Multifactor Authentication

Multifactor authentication (MFA) schemes have been actively researched in order to provide secure authentication (Khan, Ali Akbar, Shahzad, Farooq, &

Khan, 2015). The use of password authentication alone is a single-factor authentication (SFA) method; however, by adding another authentication method to the authentication process, it is called multifactor authentication. Additionally, the combination of two authentication methods can be called two-factor authentication (2FA) (Marky et al., 2022). MFA is considered safer than SFA because in case one authentication method is compromised, the other method(s) will still maintain the security of the authentication (O'Gorman et al., 2005). MFA can resist many types of attacks, for example password guessing attacks and phishing attacks, better than password authentication alone (Banyal et al., 2013). With the introduction of MFA, there are now better opportunities for creating an authentication scheme that is both secure and user-friendly (Ometov et al., 2018). This addresses the main issue associated with password use: the tradeoff between security and usability.

Authentication methods are typically divided into three categories (Gunson, Marshall, Morton, & Jack, 2011):

1. What you know
2. What you have
3. What you are

The methods are based on either knowledge, ownership, or biometrics. The first method is a knowledge-based method, and it requires a piece of information that the user knows, for example username-password credentials. The second method is based on possession of a physical token used in the authentication process and a common example of this is a smartphone or an identity badge. The third method, biometrics, relies on one of the user's intrinsic properties, qualities, or abilities, and is typically a physiological feature like a fingerprint, or a behavioral feature such as a way of speaking (Gunson et al., 2011) or a way of typing text on a keyboard (Chudá & Ďurfina, 2009; Wahab, Hou, & Schuckers, 2023).

Additionally, a fourth category of authentication, "where you are", consisting of location-based authentication methods, has been discussed (Al Kabir & Elmedany, 2022; Choi & Zage, 2012). Location-based authentication methods can be used not only for one-time identification but also for continuous identification, where the person needs to stay in a certain location to maintain a proofed identity. This type of continuous identification is convenient when a user has a designated location for using an information system, and it enables applying automated security features that provide security against remote attacks (Choi & Zage, 2012).

Many MFA schemes have been suggested by various researchers. Already in 1991, Chang and Wu (1991) were the first to introduce a 2FA method combining passwords with the use of smart cards (Wang, Wang, Xu, & Guo, 2017). The two methods used together require that the user not only knows a password but also possesses a smart card (Chang & Wu, 1991). In 2008, Sabzevar and Stavrou (2008) introduced a 2FA method involving the use of a graphical password and combined it with the use of a personal handheld device. One of the recent authentication schemes, on the other hand, completely removes the need to use passwords: it consists of a combination of a biometric authentication method and an ownership-based authentication method (Al Kabir & Elmedany, 2022).

The more authentication methods are used, the more secure the authentication is found (Mohsin, Han, Hammoudeh, & Hegarty, 2017). Different authentication schemes have varying resistance against different attack types; for example, the solution of Sabzevar and Stavrou (2008) combining a graphical password and a personal device was described to resist screen recording attacks and theft of the handheld device. On the other hand, many weaknesses have been found for example regarding smart cards: despite diverse secure smart card designs have been introduced, they have often later been found to have weaknesses against certain attack types (Wang, Wang, et al., 2017). Biometric authentication systems have also been found to be vulnerable to certain types of attacks (Rui & Yan, 2019). Securing authentication data without decreasing performance is a crucial part of the authentication process (Khan et al., 2015), and biometric data is especially important to be secured because fingerprints and other biometrics cannot be changed if stolen, and, for example, a way of speaking can be copied (O'Gorman, 2003). Biometric data can therefore even be considered similar to using the same password for several services (Marky et al., 2022). Overall, every MFA system has weaknesses that could be exploited by attackers, and therefore no MFA is perfectly secure (Wang, Zhang, Zhang, & Wang, 2020). However, research shows that already two authentication methods can provide the needed security while it does not require as much resources as authentication with more than two methods would (Mohsin et al., 2017).

As was previously mentioned, authentication should be made easy for users to use (Peisert et al., 2013) which is well-considered in authentication methods that utilize smartphones. Nowadays, since the majority of people possess smartphones with diverse communication capabilities and features such as biometric sensors, it is easy to deploy authentication methods that do not require remembering a certain piece of knowledge for large groups of users (Chuat, Plocher, & Perrig, 2020). Phone-based authentication methods include, for example, the use of text messages and authentication applications (Bonneau et al., 2012). Text messages can be used to deliver one-time passwords to the user (Bonneau et al., 2012), and authentication applications downloaded on users' devices can be used as software authentication tokens which, similarly to physical hardware tokens, create tokens to be used for authentication (Parmar et al., 2022). Using mobile devices as software tokens to generate one-time passwords that are valid for a limited amount of time is cost-efficient, secure, and does not require users to carry additional physical tokens with them (Aloul et al., 2009).

There exists a large collection of different authentication methods, each of which has its own usability, deployability, and security features (Bonneau et al., 2012). Choosing the best combination of authentication methods is not simple and requires considering the context where the method will be used (Bonneau et al., 2012). Sometimes an authentication method that is perfectly secure on paper has security issues in real life (Bonneau et al., 2012; Drimer, Murdoch, &

Anderson, 2009). The most commonly used selection criteria for authentication methods are security and usability, and sometimes also the costs of a method are considered (Velásquez et al., 2018). Usability and user experience have been highlighted as important factors in how willing individuals are to adopt 2FA (Marky et al., 2022). The application or other context where the authentication method is used is also useful to consider as criteria because more critical systems require more secure authentication (O'Gorman, 2003; Velásquez et al., 2018).

One major disadvantage of MFA is that authenticating with two or more methods takes more time and effort than with one, trading usability for security (Bonneau et al., 2012; Gunson et al., 2011). When designing MFA processes, the usability and the clarity of the authentication process should be taken into consideration (Gunson et al., 2011). For example, unclear requirements for entering passcodes into an authentication application may cause confusion for users (Gunson et al., 2011). User fatigue is a common issue with MFA, especially if MFA is frequently required, although it can be managed by only demanding MFA periodically or in specific circumstances (Fathi, Salehi, & Leiss, 2015).

If users are better informed about cyber security threats and the sensitivity of the system's data, they will better understand the importance of secure passwords (Adams & Sasse, 1999; Grawemeyer & Johnson, 2011). However, it is possible that users categorize systems based on their knowledge and deem some systems more worthy of secure password practices than others (Adams & Sasse, 1999; Grawemeyer & Johnson, 2011; Stobert & Biddle, 2018). If a user believes that the system is only exposed to minor cyber threats, they may not be motivated to take protective actions. As a result, only if a user considers the account important, they put more effort into developing a strong password (Stobert & Biddle, 2018). Additionally, it has been found that password complexity rules receive better reactions than requirements to change passwords frequently, and the difference is greater if the user considers the risk to be high for the application in question (Gebauer, Kline, & He, 2011). People invest personal resources like time, money, effort, and personal relationships while using their online service user accounts (Ogbanufe, 2023), and this affects how they perceive threats related to the service and how they cope with them. Therefore, users can be encouraged to protect their account with MFA by emphasizing their investments made in the online service (Ogbanufe, 2023).

Overall, there are many challenges in maintaining and improving password security and usability. Passwords may not be able to reliably secure user accounts if they are used in the current way. Supporting users in using passwords can make services more convenient and secure, but passwords still provide only one layer of protection for the authentication process. Due to this, MFA schemes are needed to provide a more secure way to authenticate users. Designing one completely secure authentication method is exceedingly difficult, highlighting the importance of using several authentication methods. Using strong passwords in a secure manner is crucial for ensuring the protection of sensitive information, but by combining passwords with another authentication method, it is possible to achieve an even higher level of security. In the next chapter, this thesis’ case study focusing on the MFA scheme at the Jyväskylä university is presented.

5 CASE STUDY: UNIVERSITY OF JYVÄSKYLÄ

The University of Jyväskylä (JYU) is a university of around 2 800 experts and 14 300 students in Central Finland (University of Jyväskylä, n.d.-c). There are six faculties at JYU: Faculty of Humanities and Social Sciences, Faculty of Information Technology, Jyväskylä University School of Business and Economics, Faculty of Education and Psychology, Faculty of Sport and Health Sciences, and Faculty of Mathematics and Science (University of Jyväskylä, n.d.-a). This case study focuses on the students in the Faculty of Humanities and Social Sciences. In this chapter, the information technology services at JYU and the importance of data protection for the university are discussed. Then, the current MFA method available for students at JYU is described. Finally, the case study setting and the hypotheses are presented.

5.1 Information Technology Services at the University of Jyväskylä

Information technology (IT) services are a mandatory part of university studies nowadays. JYU's IT services for students in 2023 included a variety of services such as the study system Sisu, e-learning environment Moodle, video publishing platform Moniviestin, communications platform Zoom, email, computer labs, various software, printing, personal disk space, personal web page service, remote access to university's network, wireless network (WLAN) at the university, university library web services and electronic exams taken independently in a designated classroom (University of Jyväskylä, 2020, 2023d, 2023f, n.d.-b). Several Microsoft-provided services are also available, for example, Microsoft Office 365 office applications, the file hosting service Microsoft OneDrive, and the communication platform Teams (University of Jyväskylä, 2023e).

The University of Jyväskylä has rules for using its information systems and they include the rights and responsibilities of users (University of Jyväskylä, 2023c). The rules apply to everyone using the information systems, services, connections, or equipment produced or acquired by the university or to which the university has given access. The university units that own information systems ensure that the systems are administered and maintained properly, and the university takes care of the information security of the IT services. However, the users must use the IT services according to the given rules. Illegal and unauthorized activities including, for example, searching for security gaps or decrypting other users' e-mails are prohibited. Additionally, users have a duty of confidentiality regarding non-public information about the university's information systems, including their security level, features, and data content. When it comes to users' personal files and other data stored on the university-provided services, users are responsible for the content and the appropriate level of protection of the data (University of Jyväskylä, 2023c).

The IT services are intended for university-related use, but private use on a small scale is permitted as long as it does not interfere with the designated use or violate the rules (University of Jyväskylä, 2023c). Users are responsible for all their use of the services and must protect their credentials from unauthorized use. If a user notices that their credentials have been stolen, the user must notify IT services in order to terminate the user's liability for credential misuse (University of Jyväskylä, 2023c). In case one user's credentials are compromised, not only the individual but also other users and the university may be impacted. For example, internal information or confidential research data held by the user on university file storage solutions may be leaked. The attacker can also utilize the credentials for the previously listed illegal or unauthorized activities to plan a larger information security attack against the university's IT systems.

The university keeps basic information about students in its IT systems, but students themselves can choose whether they want to use the university email service for personal purposes or upload personal files to storage solutions provided by the university. Context, or the application in question, can influence the decisions of both service providers (O'Gorman, 2003; Velásquez et al., 2018) and users, and users have been observed to categorize systems and deem some more worthy of secure practices, such as the use of strong passwords (Adams & Sasse, 1999; Gebauer et al., 2011; Grawemeyer & Johnson, 2011; Riek et al., 2016). Intentionally avoiding the use of a service can also be considered a protective action (Riek et al., 2016), and students can moderate how much data they store on the university-provided services. Even non-sensitive data can be particularly important to a student, for example unfinished essays or data for a thesis, because the student may have worked a significant number of hours to create it. If files like these have not been backed up in other storage solutions, the attacker may use them in ransom attacks.

Overall, the security of university IT services and the data stored on them is critical for the university as well as for the university staff and students. Previously, the university used a combination of username and password as the only authentication method for students' user accounts. With the growing awareness that passwords are often insecure, an MFA scheme for Microsoft-provided university IT services was introduced and rolled out to all users by the end of spring 2023.

5.2 Multifactor Authentication at the University of Jyväskylä

Although SFA methods like passwords are frequently used, MFA is becoming more popular and being adopted by many organizations, including the University of Jyväskylä. Using two strong authentication techniques helps to protect university user accounts and their data from threats such as data breaches and unauthorized access (University of Jyväskylä, 2022a). The widely used MFA scheme that combines one knowledge-based and one ownership-based authentication method (Velásquez et al., 2018) was chosen to be used at the University of Jyväskylä. The university's MFA scheme in the spring of 2023 consisted of username-password authentication and a software authentication token. To authenticate, the user had to first enter their username and password, and then their identity was verified using an application called Microsoft Authenticator. When using a specific device, application, or web browser, verification with the application was required only occasionally. Authentication with the application was further developed during 2023 by adding a verification number: in order to increase security, a number displayed on the login page after entering credentials was required to be entered into the Microsoft Authenticator application to successfully verify the identity.

MFA was made available to students and for voluntary adoption on November 18th, 2022, and it became mandatory in stages during the first half of 2023 (University of Jyväskylä, 2022b). The university staff had already been required to adopt MFA in 2022 (University of Jyväskylä, 2022a). Since MFA became available, students were informed via multiple emails and on the university website that MFA would become mandatory in the spring of 2023. The wordings in both English and Finnish in the emails and on the university website frequently attempted to encourage students to activate MFA as soon as possible ('pikimmiten') or immediately ('heti') to improve the security of user accounts:

> "Ota käyttöön pikimmiten!" (University of Jyväskylä, 2023b)

> "Please enable it as soon as possible" (University of Jyväskylä, 2023a)

> "Ottamalla monivaiheisen tunnistautumisen käyttöön heti parannat tietoturvaasi ja varmistat pääsysi tarpeellisiin tiedostoihin ja ohjelmiin." (University of Jyväskylä, 2023b)

> "The University recommends you to enable MFA as soon as possible to improve your personal data security." (University of Jyväskylä, 2023a)

Students had the option to follow the guidance and activate MFA as soon as they could, or to ignore the messages for the time being. However, during the spring of 2023, MFA became mandatory, and students were ultimately forced to activate MFA for their user accounts.

5.3 Hypotheses

This case study focuses on two groups of students: those who had voluntarily activated MFA for their university user account at the time of the study and those who had not yet activated it. According to research related to PMT, several constructs affect the intentions to use different coping strategies when faced with a threat. People with higher coping appraisal have been found to be more motivated to act adaptively, such as by using MFA, and people with higher threat appraisal have been found to be more inclined to act maladaptively (Floyd et al., 2000). It can therefore be proposed as a set of hypotheses that there are differences between students who have and who have not activated MFA for their university user account. Next, the hypotheses formed on the basis of the literature review presented earlier in this work are introduced.

Being knowledgeable about cyber threats helps in being more aware of them and protecting oneself from them, but it may not encourage people to act more securely (Kovačević et al., 2020). Knowledge can have varying and even unintended effects on information security behavior (Sheng et al., 2010). User's perception of whether they have the required knowledge about cyber security has been found to affect protection motivation negatively (De Kimpe et al., 2022). Another study that focused on a certain kind of knowledge, Greet IT knowledge, found the opposite: there was a positive correlation between perceived Green IT knowledge and Green IT adoption intention (Rochat & Ragot, 2022). To investigate if there is a difference in perceived knowledge of internet risks between students who have activated MFA and students who have not activated it, the following hypothesis is suggested:

> *H_1*: There will be a significant difference in perceived knowledge of internet risks between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Being overly optimistic about one's safety online may make it feel unnecessary to perform online safety measures (De Kimpe et al., 2022), and culture can also affect how people perceive online security threats (Chen & Zahedi, 2016). Trust has been found to reduce the level of perceived risk (Pavlou, 2003) and to correlate with the level of threat severity and vulnerability felt (De Kimpe et al., 2022). People who trust that the internet is secure have been found to not consider internet threats to be serious and to not feel that they are at risk when using the internet (De Kimpe et al., 2022). It is, however, not clear if there exists a relationship between trust and protection motivation. De Kimpe et al. (2022)

found them not to be linked, but on the other hand, Chen et al. (2022) found trust to influence adaptive coping behavior but not maladaptive coping behavior. To research if there is a difference in trust in internet safety, the following hypothesis is formed:

> *H₂*: There will be a significant difference in trust in internet safety between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Threat appraisal involves evaluating the severity and the vulnerability of a threat (Floyd et al., 2000; Rogers, 1975). Previous research on the effect of perceived severity and perceived vulnerability on protection motivation has presented contradictory results. On the one hand, they have been found to increase protection motivation (Dang-Pham & Pittayachawan, 2015; De Kimpe et al., 2022; Herath et al., 2014), but on the other hand, they have not been found to have a direct effect on use intentions (Mwagwabi et al., 2018). A high level of perceived severity may not make people feel motivated to protect themselves from information security threats if they, for example, believe that they are knowledgeable about these threats and thus feel less exposed to them (De Kimpe et al., 2022). To find out if there is a difference in the perceived severity and perceived vulnerability, the following hypotheses are suggested:

> *H₃*: There will be a significant difference in perceived severity of the threat of university user account being hacked between students who have voluntarily activated MFA for their university user account and those who have not activated it.

> *H₄*: There will be a significant difference in perceived vulnerability of the threat of university user account being hacked between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Fear appeals have been used to stir protection motivation in users (Johnston et al., 2015; Vance et al., 2022). The effect of fear appeals has, however, not been confirmed in the field of information security and might not be uniform between users (Johnston et al., 2015). Nevertheless, fear of threat has been found to influence use intentions (Mwagwabi et al., 2018; Zhang & McDowell, 2009), although the effect may be indirect (Rogers, 1975). Therefore, it is hypothesized:

> *H₅*: There will be a significant difference in fear of the threat of university user account being hacked between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Coping appraisal has been found more important in terms of enhancing information security compliance than threat appraisal (Mwagwabi et al., 2018). If, for example, complying with the information security policies is considered troublesome, people may not be willing to comply with them (Herath & Rao, 2009). Coping appraisal is essentially linked with the evaluation of adaptive behavior (Chenoweth et al., 2019). In this research, two forms of adaptive behavior are researched: the use of MFA and the use of strong passwords. Adaptive behavior has been found to be promoted by high response efficacy (Floyd et al., 2000; Herath & Rao, 2009; Mwagwabi et al., 2018; Zhang & McDowell, 2009) and high self-efficacy (Floyd et al., 2000; Mwagwabi et al., 2018), and discouraged by high response costs (Floyd et al., 2000; Zhang & McDowell, 2009). To investigate if there are differences in MFA coping appraisals and in password coping appraisals between students who have activated MFA and students who have not activated it, the three constructs, response efficacy, self-efficacy, and response costs, are examined in this study. It is therefore suggested:

> H_{6a}: There will be a significant difference in MFA response efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.
>
> H_{6b}: There will be a significant difference in MFA self-efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.
>
> H_{6c}: There will be a significant difference in MFA response costs between students who have voluntarily activated MFA for their university user account and those who have not activated it.
>
> H_{7a}: There will be a significant difference in password response efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.
>
> H_{7b}: There will be a significant difference in password self-efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.
>
> H_{7c}: There will be a significant difference in password response costs between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Adaptive behavior consists of useful ways to constructively protect oneself from a threat (Chenoweth et al., 2019), and as mentioned earlier, this research examines two forms of adaptive behavior: MFA and strong passwords. To see if there is a difference in the intention to use strong passwords between people who already use MFA as an adaptive way of behaving and people who do not use it, the following hypothesis is formed:

> H_8: There will be a significant difference in strong password use intention between students who have voluntarily activated MFA for their university user account and those who have not activated it.

A high threat appraisal may make people act maladaptively, especially when combined with a low coping appraisal (Chenoweth et al., 2019). Overlooking the possibility of maladaptive coping can be risky as some people may end up responding to threats in insecure ways (Chenoweth et al., 2019). One form of maladaptive coping is defensive avoidance where people, for example, disregard that their user account can be vulnerable to hacking (Xie et al., 2022). Therefore, in addition to the two forms of adaptive coping, one form of maladaptive coping, defensive avoidance, is examined through the following hypothesis:

> *H_9*: There will be a significant difference in defensive avoidance between students who have voluntarily activated MFA for their university user account and those who have not activated it.

6 METHODOLOGY

In the empirical part of this thesis, university students' perceptions and coping behaviors regarding securing their user accounts at the University of Jyväskylä are researched through an online survey. Three coping strategies were selected for examination: MFA, strong passwords, and defensive avoidance. The two first ones, MFA and strong passwords, are included in the study since they are currently in use at the case organization. Since the possibility of maladaptive behavior related to information systems should be more frequently considered (Chenoweth et al., 2019), defensive avoidance as one form of maladaptive behavior was chosen for examination. In the current study context, defensive avoidance refers to avoiding thinking of the possibility that someone could hack into one's university user account. The threat of hacking refers to hackers with criminal intentions gaining unauthorized access to user accounts. The research topic was narrowed to user accounts being hacked due to the interest in data breaches caused by criminal activity aroused by the media. MFA was promoted to students during a several-month-long transition period, and it became mandatory in phases by the end of April 2023. Defensive avoidance was appropriate to consider in this study because users had the option to disregard the security risks posed to their account for several months despite being advised to apply an additional security measure, MFA, for their user account.

In this chapter, the methodology of the empirical study is described. First, the participants of the survey study are introduced. Then the measures with example questions are presented. Following that, details of the pilot study and the main study are described. Finally, the procedure for how the study was run is presented.

6.1 Participants

The target group of this study consists of Jyväskylä University students in the Faculty of Humanities and Social Sciences who were the last ones for whom MFA activation became mandatory in the spring of 2023. They form one of the end user groups that use university IT services. This target group was chosen because end users, who are often seen as the weakest link in information security, have been understudied (Crossler et al., 2013; Datta et al., 2022; Schneier, 2015) despite the fact that information security heavily depends on them (Rhee et al., 2009). Furthermore, university students are mostly young adults, and younger people have been found to be more prone to fall victim to cybercrime compared to older people (Debb et al., 2020; Sheng et al., 2010; Whitty et al., 2015).

The sample was allocated into two groups: those who had voluntarily activated MFA for their university user account and those who had not yet activated it at the time of the study. If the student had not activated MFA, they used only the combination of username and password to gain access to their user account. The purpose of the study is to research whether there are differences in online security perceptions and intentions to use two other coping methods between students who had voluntarily activated MFA for their university user account and those who had not done it.

In the accepted final data, there are 48 participants' responses. In TABLE 1, the summary of the 48 accepted respondents' MFA use and demographics including age, gender, and highest education are presented. Each of these questions had a predefined set of options. Participants' ages were collected using age ranges rather than precise ages, promoting anonymity. No other personally identifiable information was collected in the interest of anonymity.

Most respondents were under 35 years old (85,4%). 18 respondents (37,5%) had already enabled MFA for their JYU user account and 30 respondents had not done it (62,5%). There were no significant differences in the demographics between the two studied groups. There was a small, not significant difference in the studied groups' age distributions: most students who had not activated MFA belonged to the age group of 18 to 24 (60%) whereas most students who had activated MFA belonged to the age group of 25 to 34 (52,9%). There were clearly more female respondents (68,8%) than male respondents (14,6%). This aligns with the gender distribution in the field of humanities, where in 2019 there were 68,9% female students and 31,1% male students, and in the field of social sciences, where there were 70% female students and 30% male students (Tilastokeskus, 2021).

TABLE 1 Accepted Respondents' Multifactor Authentication Use and Characteristics

Variable	Option	Count	Percentage
I have already enabled multifactor authentication (MFA) for my Jyväskylä University (JYU) user account.	Yes	18	37,5%
	No	30	62,5%
	Total	48	100,0%
Age	18-24	24	50,0%
	25-34	17	35,4%
	35-44	1	2,1%
	45-54	5	10,4%
	55-64	1	2,1%
	65 or over	0	0,0%
	Total	48	100,0%
Gender	Male	7	14,6%
	Female	33	68,8%
	Other	7	14,6%
	Would rather not say	1	2,1%
	Total	48	100,0%
Highest education	Comprehensive school	0	0,0%
	Upper secondary school or vocational school	18	37,5%
	Bachelor's degree	23	47,9%
	Master's degree	7	14,6%
	Doctorate degree	0	0,0%
	Total	48	100,0%

Additionally, data for previous data breach experience was collected with a set of three questions (Experience1-3) modified from the questions presented by Mousavi, Chen, Kim and Chen (2020). For example, the question for item Experience1 was "I was a victim of a data breach." and it was adapted from the original question "I was a victim of an invasion of privacy." One third of the respondents (35,4%) had some previous data breach experience. Both groups mostly disagreed on having previous data breach experience, and the MFA group disagreed slightly more than the SFA group (mean value 1,7 for the MFA group and 2,32 for the SFA group).

Those who had not activated MFA were additionally asked whether they had the intention to activate it in the next four weeks, which was before it would become mandatory. These three questions related to MFA behavioral intention (MfaBeInt1-3) were adapted from the study by Johnston & Warkentin (2010) and were included in the research purely out of interest to see if those respondents who had not yet activated MFA for their university user account were planning to do so. For example, the item MfaBeInt1 was "I intend to use multifactor authentication for my university user account in the next 4 weeks." and it was adapted from the original question "I intend to use anti-spyware software in the next 3 months." The mean value for the responses was 3,29 which is close to the neutral answer 3 of neither agreeing nor disagreeing. Therefore, the group was only very slightly inclined to agree on activating MFA. The results of this construct may have been affected by the possibility that some students can belong to many faculties of the university, and therefore they would be forced to activate MFA earlier than other students in the Faculty of Humanities and Social Sciences.

6.2 Measures

To assess the hypotheses, an online survey was conducted. The survey gathered data on students' perceptions, use of MFA, and intentions to use two other coping methods regarding securing their university user account. The online survey was sent to student email lists which reached the target group of university students well, and it was convenient that the participants could answer the survey at a time that suited them. Online surveys enable the researcher and the participant to maintain distance from one another, enhancing the impartiality of the research process (Vilkka, 2007).

The study constructs are presented in TABLE 2. Every construct has been described in detail earlier in the literature part.

TABLE 2 Summary of Constructs Used in the Current Study

Construct	Explanation in the current study context
Perceived Knowledge	Individual's thinking about whether they have the needed amount of information about threats located online and how to protect themselves from these threats (De Kimpe et al., 2022)
Internet Trust	Individual's perception of safety related to online activities and how strongly the individual believes that the internet is safe (De Kimpe et al., 2022)
Perceived Severity	Perception of how serious or severe the threat is, including evaluation of the potential harm that can come from it (Floyd et al., 2000; Rogers, 1975)
Perceived Vulnerability	Likelihood of being affected or harmed by the threat (Floyd et al., 2000; Rogers, 1975)
Fear	Emotional state connected with a threat that influences cognitive processes (Rogers, 1975)
Multifactor Authentication / Password Response Efficacy	Belief that using the coping strategy will be effective in reducing the threat (Maddux & Rogers, 1983)
Multifactor Authentication / Password Self-Efficacy	Belief that one is capable of performing the adaptive action successfully (Floyd et al., 2000)
Multifactor Authentication / Password Response Costs	The costs effective when a person takes the adaptive coping action, for example the loss of money, time, or effort (Floyd et al., 2000)
Multifactor Authentication / Password Behavioral Intention	Making the decision to start, continue, or stop implementing a coping strategy (Floyd et al., 2000)
Defensive Avoidance	Disregarding that one's user account can be vulnerable to hacking (Xie et al., 2022)

Validity refers to how well the data represents what it is believed to represent (Punch, 2003). In order to ensure a high level of validity and reliability of the measurement items, items that have been validated previously were mostly used. The wording of the items was adapted as necessary to the context of cyber security and authentication methods. Typically, each measured construct was measured by three questions. In the pilot study, all sets had two to four questions. In the main study, sets of three or four questions were used. The reason for having several similar or almost identical questions was to ensure that the questions measure the constructs reliably.

TABLE 3 describes the measured constructs, items, and examples of questions. The full lists of questions are found in APPENDIX 1 for pilot survey items and APPENDIX 2 for main survey items. The lists present the constructs, the respective items, the respective questions used in the survey, and the original questions along with their sources. Many of the chosen survey items were already suitable for the current study. Therefore, many of the items were directly taken from other studies without the need for modifications. Several items developed by De Kimpe et al. (2022) were used: two measurement items for Perceived Knowledge in the context of internet risks, three measurement items for Internet Trust, and three items for Perceived Vulnerability.

Three items for Perceived Severity and four items for Fear from the PMT-focused study by Ng et al. (2021) were used. The chosen questions focused on the individuals' own perceptions and security of personal data. For example, the wording of the questions related to the construct Perceived Severity was "… it would affect me …" which emphasizes the personal consequences. Similar items with different wording exist in the literature: Johnston and Warkentin (2010) use the wording "… it would be …" which is in passive voice, and it does not define to whom the consequences affect.

For MFA and passwords related items, the survey form asked the respondents to rate all the items "in the context of protecting your user account and data at the Jyväskylä university". Therefore, each question did not need to mention this separately. For MFA items, three items for Response Efficacy from the study by Johnston and Warkentin (2010) were adapted to fit the context of MFA. From the PMT-focused study by Ogbanufe (2023), the four items for Self-Efficacy and three items for Response Costs were used, and some of them were slightly adapted to fit the context of protecting a university user account.

For password items, three items for Response Efficacy and three items for Response Costs from the study by Zhang and McDowell (2009) were taken and partly adapted to the context of university user accounts. The four items for Self-Efficacy were taken from the password compliance study by Mwagwabi et al. (2018). Three items for Behavioral Intention from the study of Johnston and Warkentin (2010) were adapted to fit the context of passwords. Finally, the items for Defensive Avoidance were adapted to the context of university user account from the study by Chenoweth et al. (2019).

TABLE 3 Survey Constructs, Items, and Examples of Questions

Construct	**Item**	**Example question**	**Source / Adapted from**
Perceived Knowledge	PercKnow1 PercKnow2 PercKnow3	PercKnow1: I feel adequately informed about the risks of the internet.	De Kimpe et al., 2022; PercKnow3 from Rochat & Ragot, 2022
Internet Trust	Trust1 Trust2 Trust3	Trust1: I am optimistic about the safety of the internet.	De Kimpe et al., 2022
Perceived Severity	PercSev1 PercSev2 PercSev3	PercSev1: If my university user account were hacked, it would affect me severely. *Original question: If my email were hacked, it would affect me severely.*	Ng et al., 2021

Perceived Vulnerability	PercVuln1 PercVuln2 PercVuln3	PercVuln1: It is possible that I will be a victim of a data breach through my university account being hacked. *Original question: It is possible that I will be a victim of cybercrime.*	De Kimpe et al., 2022
Fear	Fear1 Fear2 Fear3 Fear4	Fear1: I am worried about my university user account being hacked. *Original question: I am worried about my email being hacked.*	Ng et al., 2021
Multifactor Authentication Response Efficacy	MfaRespEff1 MfaRespEff2 MfaRespEff3	MfaRespEff3: When using multifactor authentication, my university user account is more likely to be protected. *Original question: When using anti-spyware software, a computer is more likely to be protected.*	Johnston & Warkentin, 2010
Multifactor Authentication Self-Efficacy	MfaSelfEff1 MfaSelfEff2 MfaSelfEff3 MfaSelfEff4	MfaSelfEff1: I believe I could easily activate multi-factor authentication to prevent account hacking.	Ogbanufe, 2023
Multifactor Authentication Response Costs	MfaRespCost1 MfaRespCost2 MfaRespCost3	MfaRespCost1: Using multifactor authentication on my university user account would require considerable effort. *Original question: Using multifactor authentication on my online accounts would require considerable effort.*	Ogbanufe, 2023
Password Response Efficacy	PwRespEff1 PwRespEff2 PwRespEff3 PwRespEff4	PwRespEff1: I can protect my university user account better if I use strong passwords. *Original question: I can protect my online accounts better if I use strong passwords.*	Zhang & McDowell, 2009; PwRespEff4 is an original question
Password Self-Efficacy	PwSelfEff1 PwSelfEff2 PwSelfEff3 PwSelfEff4	PwSelfEff1: I would be able to create a strong password that is difficult to hack if I had instructions on how to create a strong password.	Mwagwabi et al., 2018
Password Response Costs	PwRespCost1 PwRespCost2 PwRespCost3	PwRespCost1: If I use strong passwords, they will be difficult for me to remember.	Zhang & McDowell, 2009

Password Behavioral Intention	PwBeInt1 PwBeInt2 PwBeInt3	PwBeInt1: I intend to use a strong password for my university user account in the next 4 weeks. *Original question: I intend to use anti-spyware software in the next 3 months.*	Johnston & Warkentin, 2010
Defensive Avoidance	DefAvoi1 DefAvoi2 DefAvoi3	DefAvoi1: I try not to let the thought of my university user account being hacked enter my mind. *Original question: I try not to let the thought of spyware enter my mind.*	Chenoweth et al., 2019

The main characteristic of a quantitative study is that it examines numerical data discussing and describing the studied items and phenomena using numbers (Vilkka, 2007). Each item was measured on a five-point Likert scale, ranging from “Strongly Disagree” to “Strongly Agree”. Since some of the original scales had a different number of measurement points, it was necessary to adapt these scales to the five-point Likert scale in order to obtain consistent scales for all questions. Originally there was a seven-point Likert scale in use for PercSev, Fear, MfaSelfEff, MfaRespCost, and DefAvoi items’ questions, and a ten-point Likert scale for PwSelfEff item’s questions.

In a survey form, the questions measuring the same construct were grouped to allow participants to focus on one construct at a time, reducing the cognitive load and increasing the accuracy of responses. Asking several similar questions in a row may be confusing for the participants. However, mixing the questions may increase the risk of response bias and force participants to shift their attention more frequently, which may lead to participant confusion and frustration. When the survey questions are presented in a logical order, it is easier and quicker for the respondents to respond.

Reliability refers to how consistent the responses given by the research participants are (Punch, 2003). The research data will have high reliability if the same participants would respond to the same questions in the same way when asked the same questions at a different time (Punch, 2003). In this study, the format of the questions was standardized, and every participant was asked the questions in the same way and offered a fixed set of options to choose from. Further, the reliability of each study construct was evaluated by Cronbach’s alpha analysis which measures the internal consistency between the questions belonging to the same study construct.

6.2.1 Pilot Study

Pilot testing is recommended for any survey questionnaire unless the exact same questionnaire has already been tested in an earlier research (Punch, 2003). The required time and effort to complete the survey should be tested as well as the readability of the survey cover letter (Punch, 2003). A pilot study was therefore conducted, and 11 responses were acquired. Cronbach's alpha test was run for the survey results and Cronbach's alpha values are presented in TABLE 4.

TABLE 4 Cronbach's Alpha Values for Pilot Survey Items

Construct	Alpha value	Actions
Perceived Knowledge	.540	Add 3rd item
Internet Trust	.640	
Past Data Breach Experience	.790	
Perceived Severity	.881	
Perceived Vulnerability	.728	
Fear	.886	
Multifactor Authentication Response Efficacy	.912	
Multifactor Authentication Self-Efficacy	.902	
Multifactor Authentication Response Costs	.716	
Multifactor Authentication Behavioral Intention	.960	Reword items
Password Response Efficacy	-2.013	Add 4th item
Password Self-Efficacy	.553	
Password Response Costs	.933	
Password Behavioral Intention	.960	Reword items
Defensive Avoidance	.457	Reword 3rd item

After the pilot study analysis, two new questions were added, and several questions were modified. Three constructs had a Cronbach's alpha value that was less than .55: Perceived Knowledge, Password Response Efficacy, and Defensive Avoidance. To enhance the internal consistency of these constructs in the main study, two questions were added. First, one item from the study by Rochat and Ragot (2022) was added for Perceived Knowledge to reach the recommended amount of a minimum of three items per construct. Since no applicable additional items were found from previous studies for Password Response Efficacy construct, a fourth item was developed using the existing three items as a basis. One question for Defensive Avoidance was reworded from "I try to ignore the possibility of my university user account being hacked." to "I try to ignore the thought of my university user account being hacked." to direct the focus more to what the respondent thinks.

In addition, it was noticed that the wording of behavioral intention items needed to be modified because the survey was launched in March instead of conducting it in February as originally planned. All the questions for both MFA and password-related behavioral intentions were modified from "…in the next month" to "… in the next 4 weeks". The need for rewording items was due to the meaning of the phrase "in the next month" not being suitable for data gathering in March as MFA was planned to become mandatory in the latter half of April. By changing the questions to refer to the next 4 weeks it was possible to gather intentions to use MFA and strong passwords before MFA was to become mandatory.

6.2.2 Main Study

The main study data was collected in March 2023. The online survey form was sent to email lists that reached JYU students from the Faculty of Humanities and Social Sciences. The time to complete the survey was estimated to be 10 minutes based on the pilot study respondents' experiences. The survey participants were chosen on a convenience basis because there was no way to moderate which students completed the survey after sending the request to complete the survey to the email lists. The sample of students who responded to the survey may have biases, leaving out, for instance, students who do not closely follow their student email. The Cronbach's alpha test was run for the main study results and the values are presented in TABLE 5.

TABLE 5 Cronbach's Alpha Values for Main Survey Items

Construct	Alpha value	Actions
Perceived Knowledge	.833	
Internet Trust	.712	
Past Data Breach Experience	.851	
Perceived Severity	.939	
Perceived Vulnerability	.792	
Fear	.918	
Multifactor Authentication Response Efficacy	.862	
Multifactor Authentication Self-Efficacy	.907	
Multifactor Authentication Response Costs	.933	
Multifactor Authentication Behavioral Intention	.943	
Password Response Efficacy	.794	
Password Self-Efficacy	.813	
Password Response Costs	.845	
Password Behavioral Intention	.974	
Defensive Avoidance	.931	

All Cronbach's alpha values were above .700 which is the threshold for an acceptable level for internal consistency of a construct. Overall, most Cronbach's alpha values are higher than in the pilot study. The number of respondents in the pilot study was only 11 whereas the main study received a higher number of 48 acceptable responses which decreases the influence of one single respondent on the results. In the pilot study, there had been a clearly inconsistent value of -2.013 for Password Response Efficacy which is why a 4th item was added for this construct. However, in the main study, even the three original items were clearly more consistent than in the pilot with Cronbach's alpha value of .668.

Despite the value being higher, it does not reach the threshold of .700, and the addition of the 4th item was needed to gain a good internal consistency (.794) of the construct.

6.3 Procedure

The survey form was hosted on the Webropol Surveys platform. The survey questionnaire was designed to be as anonymous as possible to encourage honest responses, and participants were reassured of the voluntariness and confidentiality of their responses in the cover letter. When no rewards are given for responding to a survey, it is less likely that participants will lack the motivation to provide honest answers in order to obtain a reward (Vilkka, 2007). The lack of incentives or a raffle may have contributed to excluding participants who were not motivated to complete the survey conscientiously.

At the beginning of the form, the participants were explained the topic and the reasons for the study and the data collection, and they were told that by completing the survey they consented to using their answers only for research purposes. Before asking survey questions about MFA, the participants were explained what MFA is and how it is being planned to be taken into use at the University of Jyväskylä:

> Multi-factor authentication (MFA) for Microsoft services at the University of Jyväskylä becomes mandatory in phases by the end of April 2023. MFA will be required for Microsoft services and services that are connected to Microsoft sign-in. For example, using Office 365 tools such as Word, Excel, PowerPoint, Teams, and OneDrive will require MFA. Some university services, such as student email, which is currently provided by Google, will not require MFA at this time but this may change in the future.
>
> MFA means that the user who logs in to a service is validated in multiple ways. At the University of Jyväskylä, MFA requires the user to first enter their username and password, then authenticate with a smartphone application (Microsoft Authenticator). For students in the faculty of Humanities and Social Sciences (Humanistis-yhteiskuntatieteellinen tiedekunta) the MFA is planned to become mandatory in phases in the latter half of April 2023.

The questions in TABLE 6 below were used to check whether the participant belonged to the target group of the survey and whether they had already enabled MFA for their university user account. The participant had to be a student in the Faculty of Humanities and Social Sciences at the University of Jyväskylä to participate. Additionally, the participant was not supposed to have been forced to activate MFA for their JYU user account. MFA was to be made compulsory for the students in the Faculty of Humanities and Social Sciences more than four weeks after the survey, thus, if the student did not belong to several faculties, they should not have been forced to activate it yet. Voluntary activation of MFA did not influence whether the student belonged to the target group or not.

TABLE 6 Background Variables

Variable	Item	Question
Student in the faculty of Humanities and Social Sciences	HytkStudent	I am currently a student in the faculty of Humanities and Social Sciences (Humanistis-yhteiskuntatieteellinen tiedekunta) at the University of Jyväskylä. (Yes / No)
Multifactor Authentication Use	MfaUse	I have already enabled multi-factor authentication for my Jyväskylä University (JYU) user account. (Yes / No)
	MfaUseForced	Did you activate multi-factor authentication (MFA) because you were no longer able to sign into university's Microsoft services without using it? (Yes, I could not sign in and I was forced to activate MFA / No)

As described in TABLE 7 below, less than half of the participants (43,4%) had enabled MFA for their JYU user account. Five of those had been forced to activate it because they were no longer able to sign into the university's Microsoft-provided services without using it. These five participants did not belong to the target group of the study; thus, they were redirected to exit the survey and were not asked to provide any more information. All the participants were students in the Faculty of Humanities and Social Sciences at JYU.

TABLE 7 Respondents' Multifactor Authentication Use

Variable	Option	Count	Percentage
I have already enabled multi-factor authentication (MFA) for my Jyväskylä University (JYU) user account.	Yes	23	43,4%
	No	30	56,6%
	Total	53	100,0%
Did you activate multi-factor authentication (MFA) because you were no longer able to sign into university's Microsoft services without using it?	Yes, I could not sign in and I was forced to activate MFA	5	21,7%
	No	18	78,3%
	Total	23	100,0%

7 RESULTS

This chapter describes the results obtained from the empirical research data. A quantitative analysis of whether the two student groups' perceptions and intentions to use strong passwords and defensive avoidance differ was conducted based on the hypotheses presented earlier in this study. Each hypothesis has a dedicated section where the data is examined in order to support or reject the hypothesis. The two groups of the study are referred to as the multifactor authentication group (the MFA group) which is the group that had activated MFA, and the single factor authentication group (the SFA group) which is the group that had not activated MFA.

IBM SPSS 28 statistics software was used to analyze the collected data. The recommended minimum amount of respondents to a survey is 100 when using statistical research methods, and the bigger the sample, the better it represents the target group's average perceptions about the research topic (Vilkka, 2007). Only 48 responses were received to this study's survey, and this limits the statistical analysis of the data. First, it was checked that all the survey responses were valid. The electronic form required responding to all the compulsory questions and no missing values were found. Each respondent's responses were satisfactorily varying: every participant's responses included values from the low (1-2) and the high (4-5) end of the scale, and participants' standard deviations ranged from 0,83 to 1,68. Each hypothesis was tested with the Mann-Whitney U test. The two-tailed test was used to analyze whether there were statistically significant differences between the two studied groups, regardless of the direction of the difference.

7.1 Perceived Knowledge

The construct for perceived knowledge (PercKnow) measured how the respondents perceived their knowledge about the risks of the internet and how to avoid them. It is related to hypothesis *H_1*:

> *H_1*: There will be a significant difference in perceived knowledge of internet risks between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Both studied groups' mean value of the PercKnow construct is close to 4 (4,04 for the MFA group, 3,84 for the SFA group) meaning that the respondents were more inclined to agree than disagree that they are adequately informed about the risks of the internet. The MFA group agreed more than the SFA group, and the groups' mean values are 0,2 apart. The difference between the two groups is shown to be statistically not significant with the Mann-Whitney U test ($N_1 = 18$, $N_2 = 30$, $p = .500$). Thus, the hypothesis *H_1* is not supported by the test results, suggesting that there is no significant difference in perceived knowledge between students who have voluntarily activated MFA for their university user account and those who have not activated it.

7.2 Trust

The construct for trust (Trust) measured the respondents' perception of the safety of the internet. The related hypothesis *H_2* is found below:

> *H_2*: There will be a significant difference in trust in internet safety between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Both studied groups' mean value of the Trust construct is close to 2,5 (2,56 for the MFA group, 2,44 for the SFA group), signifying that the respondents were slightly more inclined to disagree than agree that the internet is safe. The SFA group disagreed slightly more than the MFA group. The difference in the groups' mean values is only 0,12, and the Mann-Whitney U test analyzes it as statistically not significant ($N_1 = 18$, $N_2 = 30$, $p = .538$). Hypothesis *H_2* is not supported by the test results suggesting that there is no significant difference in trust in internet safety between the two studied groups.

7.3 Perceived Severity

Hypothesis *H_3* for the perceived severity construct (PercSev) is related to the differences in how severe the students find the possibility of their university user accounts being hacked:

> *H_3*: There will be a significant difference in perceived severity of the threat of university user account being hacked between students who have voluntarily activated MFA for their university user account and those who have not activated it.

The mean values of PercSev show that the respondents are more inclined towards agreeing than disagreeing that university user account hacking would affect the person severely. The MFA group has a higher mean value of 3,74 than the SFA group whose mean value is 3,44. The difference between the two groups' mean values is 0,3, and the Mann-Whitney U test shows the difference is not significant (N_1 = 18, N_2 = 30, *p* = .349). The hypothesis H_3 is therefore rejected, and the perceived severity of university user account hacking is not found to be significantly different between the two studied groups.

7.4 Perceived Vulnerability

Perceived vulnerability construct (PercVuln) measured the respondents' perceptions of their vulnerability to falling victim to the hacking of their university user account. The related hypothesis H_4 is:

> H_4: There will be a significant difference in perceived vulnerability of the threat of university user account being hacked between students who have voluntarily activated MFA for their university user account and those who have not activated it.

The mean values of PercVuln are 2,72 for the MFA group and 3,03 for the SFA group. Mean values are close to 3, the answer option "Neither agree nor disagree". The MFA group is slightly inclined to disagree, and the SFA group is very slightly inclined to agree on being vulnerable. The difference between the mean values is 0,31, and the Mann-Whitney U test shows the difference is statistically not significant (N_1 = 18, N_2 = 30, *p* = .240). Based on the results, hypothesis H_4 is rejected meaning there is no significant difference in perceived vulnerability between the groups.

7.5 Fear

Hypothesis H_5 is related to the construct of fear (Fear) and how worried the respondents find it if their university user account was hacked:

> H_5: There will be a significant difference in fear of the threat of university user account being hacked between students who have voluntarily activated MFA for their university user account and those who have not activated it.

The mean values show that the students are more inclined towards disagreeing than agreeing on being worried about their university user account being hacked. For the group that had MFA activated, the mean value is 1,72, and for the SFA group, the mean value is 1,88. The SFA group has a higher value than the MFA group, and the difference between the two groups' mean values is 0,16. The Mann-Whitney U test shows the difference is not significant (N_1 = 18, N_2 =

30, p = .611). Hypothesis H_5 is therefore rejected, and the fear of university user account being hacked is not significantly different between the two studied groups.

7.6 Multifactor Authentication Response Efficacy

The first construct related to MFA is response efficacy (MfaRespEff). It measured the respondents' perceptions of MFA's effectiveness in protecting their university user account. The related hypothesis H_{6a} is:

> H_{6a}: There will be a significant difference in MFA response efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Both studied groups' mean values of the MfaRespEff construct are close to 4 (4,20 for the MFA group, 3,86 for the SFA group) signifying that the respondents were more inclined to agree than disagree on MFA being effective for protection. The MFA group has a higher mean value than the SFA group with a difference of 0,34 between the groups' mean values. The Mann-Whitney U test analyzed the difference as statistically not significant (N_1 = 18, N_2 = 30, p = .119). Hypothesis H_{6a} is not supported by the test results suggesting that there is no significant difference in MFA response efficacy between students in the two studied groups.

7.7 Multifactor Authentication Self-Efficacy

The second construct related to MFA is self-efficacy (MfaSelfEff). It measured the respondents' perceptions about their capability to use MFA for protecting their university user account. The related hypothesis H_{6b} is:

> H_{6b}: There will be a significant difference in MFA self-efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.

The mean values of the MfaSelfEff construct are 4,17 for the MFA group and 3,58 for the SFA group, signifying that the respondents were more inclined to agree than disagree on being capable of using MFA. The MFA group has a clearly higher mean value. The difference in the groups' mean values is 0,59 and the Mann-Whitney U test shows it statistically significant (N_1 = 18, N_2 = 30, p = .033, p < .05 two-tailed test). Therefore, hypothesis H_{6b} is supported by the test results suggesting that there is a significant difference in MFA self-efficacy between students in the two studied groups.

7.8 Multifactor Authentication Response Costs

The third construct related to MFA is response costs (MfaRespCost). The related hypothesis H_{6c} discusses the respondents' perceptions related to the effort required when using MFA to protect their university user account:

> H_{6c}: There will be a significant difference in MFA response costs between students who have voluntarily activated MFA for their university user account and those who have not activated it.

The MFA group was more inclined to disagree that MFA use requires too much effort with a mean value of 2,06. On the other hand, the mean value for the SFA group is 3,04 signifying that on average the respondents did not agree nor disagree whether using MFA requires too much effort. The difference in the groups' mean values is 0,98 and the Mann-Whitney U test shows it statistically highly significant ($N_1 = 18$, $N_2 = 30$, $p = .002$, $p < .01$ two-tailed test). Thus, hypothesis H_{6c} is supported by the test results suggesting that there is a highly significant difference in MFA response costs between students in the two studied groups.

7.9 Password Response Efficacy

The first construct related to passwords is response efficacy (PwRespEff). It measured the respondents' perception of strong passwords' effectiveness in protecting their university user account. The related hypothesis H_{7a} is:

> H_{7a}: There will be a significant difference in password response efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Both studied groups' mean values of the PwRespEff construct are over 4, and the SFA group has a higher mean value than the MFA group (4,28 for the MFA group, 4,57 for the SFA group). This signifies that the respondents were more inclined to agree than disagree that strong passwords are effective for protection. The difference in the groups' mean values is 0,29 and the Mann-Whitney U test analyzes it as statistically not significant ($N_1 = 18$, $N_2 = 30$, $p = .078$). Hypothesis H_{7a} is therefore not supported by the test results suggesting that there is no significant difference in password response efficacy between students in the two studied groups. The value is, however, close to being statistically significant.

7.10 Password Self-Efficacy

The second construct related to passwords is self-efficacy (PwSelfEff). It measured the respondents' perceptions of their capability to use strong passwords for protecting their university user account. The related hypothesis H_{7b} is:

> H_{7b}: There will be a significant difference in password self-efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.

The mean values for the PwSelfEff construct are 3,74 for the MFA group and 4,02 for the SFA group, signifying that the respondents were more inclined to agree than disagree that they are capable of using strong passwords. The SFA group has a higher mean value, and there was a difference of 0,28 in the groups' mean values. The Mann-Whitney U test shows the difference is statistically not significant ($N_1 = 18$, $N_2 = 30$, $p = .484$). Hypothesis H_{7b} is therefore rejected by the test results suggesting that there is no significant difference in password self-efficacy between students in the two studied groups.

7.11 Password Response Costs

The third construct related to passwords is response costs (PwRespCost). The related hypothesis H_{7c} discusses the respondents' perceptions of the effort required to use strong passwords for protecting their university user account:

> H_{7c}: There will be a significant difference in password response costs between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Both groups were inclined to agree that strong password use requires too much effort (the mean value was 3,61 for the MFA group and 3,88 for the SFA group). The SFA group has a higher mean value than the MFA group. The difference in the groups' mean values is 0,27 and the Mann-Whitney U test shows it is statistically not significant ($N_1 = 18$, $N_2 = 30$, $p = .451$). Hypothesis H_{7c} is rejected by the test results, suggesting that there is no significant difference in strong password response costs between students in the two studied groups.

7.12 Strong Password Use Intention

Strong password use intention construct (PwBeInt) measured the respondents' intention to use a strong password for their university user account. The hypothesis H_8 is:

> H_8: There will be a significant difference in strong password use intention between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Both groups were inclined to agree that they intended to use strong passwords, but the MFA group has a bit lower mean value (the mean value is 3,59 for the MFA group and 3,76 for the SFA group). The difference between the mean values is 0,17 and the Mann-Whitney U test shows it is statistically not significant (N_1 = 18, N_2 = 30, p = .639). Based on the results, hypothesis H_8 is rejected meaning there is no significant difference in strong password use intention between the two groups of students.

7.13 Defensive Avoidance

The construct for defensive avoidance (DefAvoi) measured the respondents' intention to avoid thinking of the thought of their university user account being hacked and hypothesis H_9 is found below:

> H_9: There will be a significant difference in defensive avoidance between students who have voluntarily activated MFA for their university user account and those who have not activated it.

Both studied groups' mean values of the DefAvoi construct are close to 3,5 (3,65 for the MFA group, 3,42 for the SFA group), signifying that the respondents were more inclined to agree than disagree that they avoid thinking their university user account being hacked. The MFA group has a higher mean value than the SFA group. The difference in the groups' mean values is 0,23 and the Mann-Whitney U test analyzed it statistically not significant (N_1 = 18, N_2 = 30, p = .620). Hypothesis H_9 is not supported by the test results suggesting that there is no significant difference in defensive avoidance between students in the two studied groups.

7.14 Summary

The summary of the descriptive statistics for the study constructs is provided in TABLE 8. For most of the constructs, the mean values of the two groups are at most 0,35 apart. The mean values varied more from each other only in the case of Multifactor Authentication Self-Efficacy (0,59) and Multifactor Authentication Response Costs (0,98).

TABLE 8 Descriptive Statistics for Study Constructs

Construct	**MFA group**		**SFA group**	
	Mean	Standard Deviation	Mean	Standard Deviation
Perceived Knowledge	4,04	0,63	3,84	0,87
Internet Trust	2,56	0,84	2,44	0,74
Perceived Severity	3,74	0,76	3,44	0,99
Perceived Vulnerability	2,72	0,86	3,03	0,91
Fear	1,72	0,73	1,88	0,88
Multifactor Authentication Response Efficacy	4,20	0,65	3,86	0,60
Multifactor Authentication Self-Efficacy	4,17	0,72	3,58	0,97
Multifactor Authentication Response Costs	2,06	0,79	3,04	1,12
Password Response Efficacy	4,28	0,59	4,57	0,48
Password Self-Efficacy	3,74	1,03	4,02	0,79
Password Response Costs	3,61	1,16	3,88	1,03
Password Behavioral Intention	3,59	1,03	3,76	1,01
Defensive Avoidance	3,65	0,93	3,42	1,11

TABLE 9 summarizes the inferential statistics for the study constructs. Two of the constructs, Multifactor Authentication Self-Efficacy and Multifactor Authentication Response Costs, had a significant difference between the mean values of the two studied groups examined by the Mann-Whitney U test (N_1 = 18, N_2 = 30, p < .05 two-tailed test). None of the other constructs had a significant difference between the mean values of the two studied groups examined by the Mann-Whitney U test (N_1 = 18, N_2 = 30, p > .05 two-tailed test).

TABLE 9 Inferential Statistics for Study Constructs

Construct	**Hypothesis**	**U**	**Sig. (two-tailed test)**
Perceived Knowledge	*H_1*	239,00	0,500
Internet Trust	*H_2*	241,50	0,538
Perceived Severity	*H_3*	226,50	0,349
Perceived Vulnerability	*H_4*	324,50	0,240
Fear	*H_5*	293,50	0,611
Multifactor Authentication Response Efficacy	*H_{6a}*	199,00	0,119
Multifactor Authentication Self-Efficacy	*H_{6b}*	171,00	0,033*
Multifactor Authentication Response Costs	*H_{6c}*	414,50	0,002**
Password Response Efficacy	*H_{7a}*	349,00	0,078
Password Self-Efficacy	*H_{7b}*	302,50	0,484
Password Response Costs	*H_{7c}*	305,00	0,451
Password Behavioral Intention	*H_8*	291,50	0,639
Defensive Avoidance	*H_9*	247,00	0,620

* significant

** highly significant

TABLE 10 summarizes the support of the hypotheses. Two hypotheses, H_{6b} and $H_{6c,}$ were supported. Hypothesis H_{6b} examined the Multifactor Authentication Self-Efficacy and hypothesis H_{6c} considered the Multifactor Authentication Response Costs. The rest of the hypotheses were not supported.

TABLE 10 Hypotheses and Their Support

Hypothesis	**Supported**
H_1: There will be a significant difference in perceived knowledge of internet risks between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_2: There will be a significant difference in trust in internet safety between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_3: There will be a significant difference in perceived severity of the threat of university user account being hacked between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_4: There will be a significant difference in perceived vulnerability of the threat of university user account being hacked between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_5: There will be a significant difference in fear of the threat of university user account being hacked between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_{6a}: There will be a significant difference in MFA response efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_{6b}: There will be a significant difference in MFA self-efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.	Yes
H_{6c}: There will be a significant difference in MFA response costs between students who have voluntarily activated MFA for their university user account and those who have not activated it.	Yes
H_{7a}: There will be a significant difference in password response efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_{7b}: There will be a significant difference in password self-efficacy between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_{7c}: There will be a significant difference in password response costs between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_8: There will be a significant difference in strong password use intention between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No
H_9: There will be a significant difference in defensive avoidance between students who have voluntarily activated MFA for their university user account and those who have not activated it.	No

8 DISCUSSION

This study examined whether there are differences in online security perceptions regarding the threat of university user account being hacked, intentions to use strong passwords, and defensive avoidance between students who had activated MFA for their university account and those who had not activated it. In this chapter, the study findings and implications for researchers, practitioners, and the case organization, the University of Jyväskylä, are discussed. Finally, the limitations of this study and suggestions for future research topics are presented.

8.1 Findings

The main finding of the study is that the studied groups had significant differences in two constructs: MFA self-efficacy and MFA response costs. This answers the first research question related to the differences in online security perceptions. Adaptive behavior such as the use of MFA has been found to be promoted by high self-efficacy (Floyd et al., 2000; Mwagwabi et al., 2018), and as the MFA group had a higher mean value of this construct than the SFA group, the results align with prior studies. High response costs, on the other hand, have been found to discourage adaptive behavior (Floyd et al., 2000; Zhang & McDowell, 2009), and the results of the current study support this finding as the MFA group had a lower mean value for response costs than the SFA group.

Overall, these findings are consistent with prior research on PMT, which has found that a high level of coping appraisal encourages adaptive behavior (Chenoweth et al., 2019; Floyd et al., 2000). Earlier literature has stated that coping appraisal is more crucial to consider than threat appraisal when enhancing information security compliance (Mwagwabi et al., 2018), which aligns with the study findings where the only significant differences between the studied groups were found in the coping appraisal constructs.

Apart from the two mentioned differences, the two studied groups had quite similar online security perceptions. There was no difference in one of the coping appraisal constructs: MFA response efficacy. Adaptive behavior has been previously found to be promoted by high response efficacy (Floyd et al., 2000; Mwagwabi et al., 2018; Zhang & McDowell, 2009), meaning that the current study results differ from prior research. Both groups considered MFA to be effective for protecting their user account, yet not everyone had activated it.

The respondents held similar opinions about how well-informed they felt they were about the risks associated with using the internet and how satisfied they were with internet security. These findings are not consistent with previous research. The two concepts, perceived knowledge and trust, have not been extensively studied as antecedents of threat and coping appraisals, but perceived knowledge has previously been found to correlate directly with protection motivation (De Kimpe et al., 2022). There have been differing study results on trust, and it has been associated with protection motivation directly (Chen et al., 2022) and indirectly through its constructs (De Kimpe et al., 2022), for example by reducing the level of perceived risk (Pavlou, 2003).

Knowledge about cyber security risks and protection methods does not necessarily encourage individuals to act against threats. Overall, knowledge has been found to help in protection against cyber security risks (Kovačević et al., 2020), and knowledgeable experts in online security such as computer science students or professionals have been found to have stronger passwords than non-experts such as business school users (Mazurek et al., 2013). In the current study, if perceived knowledge about MFA had been examined instead of perceived knowledge about the risks of the internet, the results could have been different. For example, in the study by Rochat and Ragot (2022), the respondents who had a high level of perceived knowledge about Green IT had a higher adoption intention of Green IT than respondents with a lower level of Green IT knowledge. Awareness of risks may not be linked to the risks of falling victim to phishing (Vishwanath et al., 2011), but training against an attack type such as cue-based training against phishing emails has been proven useful (Sturman et al., 2023). Therefore, more specific knowledge may have a different impact than overall knowledge about cyber security risks which could explain the current study results.

There was no statistically significant difference found in the threat appraisal constructs of perceived severity and perceived vulnerability between the groups. Both groups held similar opinions regarding how serious or likely they believed the risk of having their university user account hacked to be. In prior research, higher levels of perceived severity (Dang-Pham & Pittayachawan, 2015) and perceived vulnerability (De Kimpe et al., 2022) have been suggested to motivate protection motivation, particularly in the case of maladaptive coping behavior (Floyd et al., 2000). However, in the current study, threat appraisal levels were close to neutral or slightly elevated for both groups, indicating that their influence may have been minimal. Prior research is also ambiguous about the effect of threat appraisal in the context of information security, and threat appraisal constructs may not always be directly related to use intentions (Mwagwabi et al., 2018). As cybercrimes often have unclear consequences (Woods & Walter, 2022), it may be challenging to see the value in taking protective measures even though a person is aware that there is a high risk. Overall, the current study supports the notion that further research is needed to clarify the effects of threat appraisal in the context of information security.

Fear of one's university user account being hacked did not differ statistically between the studied groups. The findings are consistent with earlier research, which has demonstrated that while fear has an indirect effect through the cognitive processes described in PMT, it does not directly affect use intentions (Rogers, 1975). Additionally, there has been discussion concerning the effectiveness of fear appeals in the field of information security (Johnston et al., 2015), for example, because not all end users are equally influenced by them (Johnston & Warkentin, 2010).

The intention to use strong passwords and defensive avoidance were found to be at similar levels in both studied groups. Thus, the answer to the second and the third research questions is that there were no differences between the studied groups regarding these two coping mechanisms. Defensive avoidance as one form of maladaptive coping (McCrae, 1984) did not differentiate the two studied groups: both groups gave slightly positive answers when asked whether they try not to think about their account being hacked. Since neither threat appraisal nor defensive avoidance varied between the studied groups in this study, the study findings are consistent with earlier studies that link maladaptive behavior to an elevated perception of threat (Floyd et al., 2000; Xie et al., 2022). Password-related coping appraisals were also on similar levels in the responses of the two groups, although password response efficacy was close to the statistical difference between the two groups. When asked if they could protect their university user account with strong passwords, the respondents who used SFA agreed slightly more on average than those who had activated MFA. Overall, the results showing the same level of password-related coping appraisal and similar intentions to use strong passwords align with prior studies that link coping appraisal to adaptive behavior (Chenoweth et al., 2019; Floyd et al., 2000).

Additionally, the differences between MFA and password coping appraisals provide some intriguing insights. The MFA group had high mean values of over 4 for both coping mechanisms' response efficacy while the SFA group had a lower mean value of 3,86 for MFA response efficacy and a higher mean value of 4,57 for password response efficacy. Therefore, the SFA group believed that using strong passwords is slightly more effective in protecting their university user account than using MFA. Results on self-efficacy constructs show that the MFA group felt slightly more capable of using MFA (mean value of 4,17) than strong passwords (mean value of 3,74), while on the contrary, the SFA group thought that they were slightly more capable of using passwords (mean value of 4,02) than MFA (mean value of 3,58). Both groups agreed that password response costs are higher (mean value for the MFA group was 3,61 and for the

SFA group it was 3,88) than MFA response costs (mean value for the MFA group was 2,06 and for the SFA group it was 3,04).

Average password strength has been found weak in previous studies (Bonneau, 2012; Vu et al., 2007) making it a rather weak authentication method (Vu et al., 2007). In the combined responses from both groups, the intention to use strong passwords was positive (mean value of 3,68), and the password response efficacy was high (mean value of 4,43). However, the password response costs were found to be slightly high (mean value of 3,75) which indicates that people may find using strong passwords burdensome. Thus, even though strong passwords are found effective in protection, users may not have strong intentions to use them in practice because it requires effort.

According to the collected data, there were no significant differences in the demographics or past data breach experience between the studied groups. There was a small yet not significant difference in experience: the MFA group agreed slightly less on having data breach experience than the SFA group. To date, the role of experience remains unclear. Experiencing cybercrime has been found not to have an effect on how non-experts evaluate the possibility of online hazards (Creese et al., 2013), but experiencing cybercrime may increase avoidance of using online banking and social networking services (Riek et al., 2016). Previous research has additionally shown that a person's gender and level of education can have moderate to no impact on their victimization by cybercrime (Sheng et al., 2010), but in the current study, the studied groups did not have significant differences in these demographics. However, contrary to earlier studies, the current study discovered that the age variable did not vary between the two groups. Younger people are more likely to become victims of cybercrime (De Kimpe et al., 2022; Debb et al., 2020; Sheng et al., 2010) due to risk factors such as being overoptimistic while utilizing online services (De Kimpe et al., 2022) and having less knowledge about information security (Debb et al., 2020; Sheng et al., 2010). Nevertheless, it is reasonable that there was no significant difference discovered in the current study because the sample population of university students consisted of very even-aged students and the respondents were primarily under the age of 35.

8.2 Research Implications

The results of this study suggest that people who voluntarily activate MFA do not have any higher perceptions of threat nor more knowledge, but they do have a higher level of coping appraisal. Similarly in previous research, it has been found that security threats do not always motivate action, and thus usability should be on a good level to enhance protection motivation (Gunson et al., 2011). For some individuals, threats may feel less concerning than for others (Haag et al., 2021), and in the current study, the fear of one's user account being hacked was not found to differ between students who had protected their account through activating MFA and those who had not done so. The level of concern about security breaches does not imply that people would act; they also need to be informed that the effort used to take a security measure has a positive impact (Herath & Rao, 2009).

All in all, information systems are dependent on people, and therefore protection requires more than just a strong technical solution; it also needs to be easy to use and have a clear purpose (West et al., 2009), highlighting the importance of coping appraisal. End users as the weakest point in information security (Crossler et al., 2013; Schneier, 2015) are important to consider in online services (West et al., 2009), particularly when the services are targeted for a large number of end users from diverse backgrounds and with varying technical skills. As it has been important to take user behavior into account in the past (Adams & Sasse, 1999), it will also be important in the future. Because people have been found to be reluctant to comply with troublesome policies (Herath & Rao, 2009), making the use of MFA or other protective measures easier can raise the number of people willing to use them.

8.3 Practical Implications

In this case study about securing university user accounts, the capability to perform a security measure and the costs of performing it were the factors that differentiated the two groups of students. Balancing between security and usability has been a challenge in the use of passwords as an authentication method (Adams & Sasse, 1999; Guo et al., 2019), and the struggle continues with other authentication methods (Fathi et al., 2015; Gunson et al., 2011; Velásquez et al., 2018). With passwords, users try to find the easiest and often unsafe ways to follow the rules (Guo et al., 2019; Vu et al., 2007) and utilize coping strategies to deal with the rules (Adams & Sasse, 1999; Siponen et al., 2020; Stobert & Biddle, 2018). Therefore, security and usability are both important when choosing authentication methods for services (Velásquez et al., 2018).

Supporting users in the use of the chosen authentication methods makes their use easier and more appealing. Technology systems often support the culture of poor password management (Gaw & Felten, 2006), and thus information system designers should plan how to support users in using secure authentication methods. One major disadvantage of MFA is that authenticating with two or more methods takes more time and effort than with one, trading usability for security (Bonneau et al., 2012; Gunson et al., 2011). Demanding MFA only periodically is seen as a way to manage user fatigue (Fathi et al., 2015). This practice is also in use at the University of Jyväskylä, improving usability and reducing the effort required to use MFA.

Overall, combining both technical measures and non-technical measures is crucial in lowering the risk of cyberattacks (Heartfield & Loukas, 2015), and by increasing understanding of individuals' behavior, it is easier to involve them in securing information systems (Crossler et al., 2013). Data breaches can cause significant losses for organizations and individuals (Sen & Borle, 2015). By understanding the end users, it is possible to improve security for organizations, which in turn can help in reducing security breaches, reputational damages, and financial losses that cybercrime can cause.

8.4 Case Study Implications

The University of Jyväskylä had been informing students by sending several emails about the Microsoft MFA becoming mandatory in Spring 2023. However, many students had not enabled MFA even though at the time of the survey it had been possible for over 3 months (University of Jyväskylä, 2022b). Even though knowledge can motivate and help in protection against cyber risks (Creese et al., 2013; De Kimpe et al., 2022; Kovačević et al., 2020; Mazurek et al., 2013), it alone does not necessarily lessen the risks of victimization (Vishwanath et al., 2011). Emphasizing investments made in an online service can motivate MFA adoption (Ogbanufe, 2023), and for example, telling students what needs to be protected and why can help them make the decision of whether to apply additional safeguards for their user account or not.

Since the lack of understanding about password security can sometimes make it difficult to use strong passwords (Ur et al., 2016), training on authentication methods can be useful (Furnell et al., 2018; Grawemeyer & Johnson, 2011), especially for the most vulnerable users (Albladi & Weir, 2018). At the University of Jyväskylä, it can be useful to train users on authentication methods so that the users can more easily use the authentication tools. The security of user accounts is important to the university, because when an account is hacked, not only the users' data but also the university's data can be leaked. Additionally, the attacker can also gain access to the university's services that are only allowed to be used by university staff and students. Currently, no mandatory training is required on authentication methods, but information and help are available from IT support. Since discussing the topic is currently topical and meaningful, conducting research and surveys about information security and authentication methods can also raise awareness of these topics among students.

The perceived severity was not particularly high, and the perceived vulnerability was close to indifferent in the survey data, and one explanation for this can be that the students do not consider the data stored in their university user accounts to be sensitive. The application that is being protected affects security behavior decisions (O'Gorman, 2003; Velásquez et al., 2018), and users have been found to categorize systems and deem some more worthy of secure practices such as using strong passwords (Adams & Sasse, 1999; Gebauer et al., 2011; Grawemeyer & Johnson, 2011; Riek et al., 2016). Since users have found security-wise questionable ways to cope with passwords, they may produce ways to circumvent the security rules of other authentication methods as well. The possibility of maladaptive behavior should therefore be considered (Chenoweth et al., 2019), and a maladaptive protective action can, for example, be the intention to avoid utilizing a service (Riek et al., 2016). Students can moderate how much data they store in the university-provided services, and if they do not store any sensitive data in the services, they may find it unnecessary to protect their user accounts well. The perceived cybercrime risk can influence avoiding online service use (Riek et al., 2016), and avoiding storing sensitive data in these services can be one option to manage the threat of account hacking.

Both studied groups were inclined to agree with the statement that they intended to use strong passwords. Even though the MFA users had to use two authentication methods, they had equal intentions to use strong passwords compared to the SFA users. Passwords are the first line of defense (Fandakly & Caporusso, 2020), but on average they are weak and often do not provide strong protection on their own (Bonneau, 2012; Vu et al., 2007). However, they can complement the use of other authentication methods. The more authentication methods are used, the more secure the authentication is considered (Mohsin et al., 2017). Professional attackers are all the time trying to find new ways to attack information systems (Huang et al., 2018), and if an attacker manages to access the user's device and the authentication application, authentication may be compromised. To maintain authentication security at a good level, it is therefore important to ensure that more than one secure authentication method is used (O'Gorman et al., 2005). If the authentication app had simply replaced passwords at the University of Jyväskylä, there would still be only one line of defense. Making MFA mandatory to use is useful for improving the security of university user accounts, but promoting other secure coping behaviors is also important. Passwords remain the most used authentication method (Bonneau et al., 2012; Gaw & Felten, 2006; Holt, 2011; Vu et al., 2007), and despite the university introducing an authentication application, passwords were not sent to retirement. Passwords continue to be an important component of authentication at the University of Jyväskylä. The strength of MFA is based on individual authentication methods, which is why it is important to highlight the importance of avoiding weak passwords in the future as well.

8.5 Limitations and Suggestions for Future Research

The small number of respondents and the precisely defined sample population prevents making broad generalizations about the study findings. The limited sample population and the absence of an incentive raffle may have contributed to the study's low response rate, limiting the generalizability to all university students. There is also a chance of nonresponse error, and only those most interested in the subject may have participated in the survey (Groves, Presser, & Dipko, 2004). Additionally, the target population of university students can vary from other citizens and other people in the same age group in a number of ways, and thus the results cannot be generalized to the wider population.

In a survey study, it is possible that the respondents do not understand the questions the way the researcher expected them to, and in a small sample size, the impact of one respondent misinterpreting a question is greater than it would be in a larger sample size. Due to the fact that the prior research literature and survey questions have been published mainly in English and that there was not enough time to translate the survey questions into Finnish, the survey questions for this study were only available in English even though the respondents were from a Finnish university. The feedback from respondents, who do not speak English as their first language, highlighted that it was confusing and challenging to understand the very similar questions in the survey. For instance, the similar adjectives "worried," "frightened," "anxious," and "scared" were used in the survey questions to measure the level of fear. Therefore, the respondents' English language skills may have had an impact on the results. In future studies, it would be wise to take into account the possible language barrier and to write survey questions in the language that the target group is most comfortable with. A survey can also be made available in multiple languages, but translating a survey entails a lot of work, such as ensuring that the questions are understood in the same way in each language and examining the internal consistency of question sets in each language.

As most research has previously concentrated on firms, there is reason to continue researching individuals' behavior related to security breaches (Ablon et al., 2016). The behavioral literature has identified over 20 different forms of maladaptive coping (McCrae, 1984), and including several of these forms in a case study could provide insightful information about how individuals respond to information security threats. In the case of university students, it would be interesting to study, for example, whether students avoid storing sensitive data in IT services provided by the university.

The emotion of fear was examined in this study; however, numerous other emotions have been studied in the past in the context of information technology (Beaudry & Pinsonneault, 2010; Wang, Li, & Rao, 2017). It would be interesting to study the emotions people experience when forced to adopt a specific technology, and how those emotions influence whether people adopt the technology voluntarily before being forced to do so. Since a 5-point Likert scale is less sensitive than a scale with more options (Rochat & Ragot, 2022), it could be useful to use a scale with more options while examining human emotions to increase the scale's sensitivity to subtle differences.

9 CONCLUSION

This thesis studied students' perceptions and coping methods regarding securing their user accounts at the University of Jyväskylä. The empirical part of the thesis presented a practical example of a case study where the existing theories of protection motivation and coping behaviors were applied in the context of information security, using the University of Jyväskylä as the case organization. The case study consisted of hypotheses formed on the basis of a literature review, and it examined whether there were differences in online security perceptions and intentions to use strong passwords or avoid thinking about the threat of one's user account being hacked between students who had voluntarily activated MFA and students who had not activated it. The research questions based on the aforementioned objectives were:

> *RQ_1*: Are there differences in online security perceptions between students who have activated multifactor authentication for their university user account and those who have not?
>
> *RQ_2*: Are there differences in students' intentions to use strong passwords regarding the threat of their university user account being hacked between those who have activated multifactor authentication and those who have not?
>
> *RQ_3*: Are there differences in students' intentions to use defensive avoidance regarding the threat of their university user account being hacked between those who have activated multifactor authentication and those who have not?

The answer to the first research question forms the main finding of the study; the studied groups had significant differences in two coping appraisal constructs, MFA self-efficacy and MFA response costs. Multiple other constructs related to perceptions regarding securing university user accounts were studied, and no significant differences were found between the two groups. Additionally, the intention to use strong passwords and defensive avoidance were found to be at similar levels in both studied groups. Thus, the answer to the second and the third research questions is that there were no differences between the studied groups regarding the two other coping mechanisms examined.

The results of this study provide insights into students' perceptions about online security and authentication methods as well as intentions to use different coping mechanisms to protect their university user accounts. The results suggest that students who voluntarily activated MFA do not have any higher perceptions of threat nor more knowledge, but they do have a better level of two coping appraisals. Considering the response costs low and the capability to do actions high were found to be more important than perceptions of the threat. It is, therefore, essential to consider how capable the users perceive themselves to be in using a specific authentication method and how much effort using the method requires from the user.

Finally, after conducting an extensive analysis of the data collected and thoroughly examining the relevant literature, it is evident that more research into coping mechanisms is needed, especially to further clarify the effects of coping and threat appraisal on individuals in the context of information security. This aligns with the existing research pointing out the need for more research, especially on the effect of threat appraisal (Johnston & Warkentin, 2010; Johnston et al., 2015) and adaptive and maladaptive coping actions (Chen et al., 2022). Unauthorized access is one of the biggest security threats (Velásquez et al., 2018), making secure authentication essential for any information system. Suggestions of new user-friendly authentication methods have been made to bypass the trouble of password memorability (Barron et al., 2021; Chuat et al., 2020), making many of the new methods easier to use for human users. Organizations can use MFA to effectively protect users from account hacking and data breaches, but the end user behavior must also be taken into consideration. Thus, human behavior and supporting users should not be forgotten when planning changes to the authentication methods used in an organization.

REFERENCES

Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. (2016). *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*. Rand Corporation.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46.

Al Kabir, M. A., & Elmedany, W. (2022). An Overview of the Present and Future of User Authentication. *2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, 10–17. https://doi.org/10.1109/MENACOMM57252.2022.9998304

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*(1), 5. https://doi.org/10.1186/s13673-018-0128-7

Aldawood, H., & Skinner, G. (2020). Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions. *IEEE Access*, *8*, 67321–67329. https://doi.org/10.1109/ACCESS.2020.2983280

Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. *2009 IEEE/ACS International Conference on Computer Systems and Applications*, 641–644. https://doi.org/10.1109/AICCSA.2009.5069395

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–643. https://doi.org/10.2307/25750694

Bang, Y., Lee, D.-J., Bae, Y.-S., & Ahn, J.-H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. *International Journal of Information Management*, *32*(5), 409–418. https://doi.org/10.1016/j.ijinfomgt.2012.01.001

Banyal, R. K., Jain, P., & Jain, V. K. (2013). Multi-factor Authentication Framework for Cloud Computing. *Modelling and Simulation 2013 Fifth International Conference on Computational Intelligence*, 105–110. https://doi.org/10.1109/CIMSim.2013.25

Barron, T., So, J., & Nikiforakis, N. (2021). Click This, Not That: Extending Web Authentication with Deception. *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 462–474. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3433210.3453088

Barton, B. F., & Barton, M. S. (1984). User-friendly password methods for computer-mediated information systems. *Computers and Security*, *3*(3), 186–195. https://doi.org/10.1016/0167-4048(84)90040-3

Beaudry, A., & Pinsonneault, A. (2010). The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use. *MIS Quarterly*, *34*(4), 689–710. https://doi.org/10.2307/25750701

Bonneau, J. (2012). The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. *2012 IEEE Symposium on Security and Privacy*, 538–552. https://doi.org/10.1109/SP.2012.49

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Chang, C.-C., & Wu, T.-C. (1991). Remote password authentication with smart cards. *IEE Proceedings E (Computers and Digital Techniques)*, *138*(3), 165–168. https://doi.org/10.1049/ip-e.1991.0022

Chen, Y., Luo, X. R., & Li, H. (2022). Beyond adaptive security coping behaviors: Theory and empirical evidence. *Information & Management*, *59*(2), 103575. https://doi.org/10.1016/j.im.2021.103575

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly*, *40*(1), 205–222.

Chenoweth, T., Gattiker, T., & Corral, K. (2019). Adaptive and Maladaptive Coping with an It Threat. *Information Systems Management*, *36*(1), 24–39. https://doi.org/10.1080/10580530.2018.1553647

Choi, S., & Zage, D. (2012). Addressing insider threat using “where you are” as fourth factor authentication. *2012 IEEE International Carnahan Conference on Security Technology (ICCST)*, 147–153. https://doi.org/10.1109/CCST.2012.6393550

Chuat, L., Plocher, S., & Perrig, A. (2020). Zero-Knowledge User Authentication: An Old Idea Whose Time Has Come. In J. Anderson, F. Stajano, B. Christianson, & V. Matyáš (Eds.), *Security Protocols XXVII* (pp. 203–212). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-57043-9_19

Chudá, D., & Ďurfina, M. (2009). Multifactor authentication based on keystroke dynamics. *Proceedings of the International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing*, 1–6. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1731740.1731836

Conklin, A., Dietrich, G., & Walz, D. (2004). Password-based authentication: A system perspective. *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of The*, 10 pp.-. https://doi.org/10.1109/HICSS.2004.1265412

Creese, S., Hodges, D., Jamison-Powell, S., & Whitty, M. (2013). Relationships between Password Choices, Perceptions of Risk and Security Expertise. In L. Marinos & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (pp. 80–89). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-39345-7_9

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

CSRC. (2022, July 21). Glossary | CSRC. Retrieved 24 August 2022, from https://csrc.nist.gov/glossary

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281–297. https://doi.org/10.1016/j.cose.2014.11.002

Datta, P., Sartoli, S., Gutierrez, L. F., Abri, F., Namin, A. S., & Jones, K. S. (2022). A user-centric threat model and repository for cyber attacks. *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, 1341–1346. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3477314.3507315

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology, 41*(8), 1796–1808. https://doi.org/10.1080/0144929X.2021.1905066

Debb, S. M., Schaffer, D. R., & Colson, D. G. (2020). A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults. *International Journal of Cybersecurity Intelligence & Cybercrime*, *3*(1), 42–55.

Drimer, S., Murdoch, S. J., & Anderson, R. (2009). Optimised to Fail: Card Readers for Online Banking. In R. Dingledine & P. Golle (Eds.), *Financial Cryptography and Data Security* (pp. 184–200). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-03549-4_11

Dupuis, M., & Khan, F. (2018). Effects of peer feedback on password strength. *2018 APWG Symposium on Electronic Crime Research (eCrime)*, 1–9. https://doi.org/10.1109/ECRIME.2018.8376210

Eurostat. (2023). *Individuals – Internet activities* [Data set]. Retrieved from https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_ac_i$dv_645/default/table?lang=en

Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., … Ome, U. (2023). Password-based authentication and the experiences of end users. *Scientific African*, *21*, e01743. https://doi.org/10.1016/j.sciaf.2023.e01743

Fandakly, T., & Caporusso, N. (2020). Beyond Passwords: Enforcing Username Security as the First Line of Defense. In T. Ahram & W. Karwowski (Eds.), *Advances in Human Factors in Cybersecurity* (pp. 48–58). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-20488-4_5

Fathi, R., Salehi, M. A., & Leiss, E. L. (2015). User-Friendly and Secure Architecture (UFSA) for Authentication of Cloud Services. *2015 IEEE 8th International Conference on Cloud Computing*, 516–523. https://doi.org/10.1109/CLOUD.2015.75

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web*, 657–666. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1242572.1242661

Florêncio, D., Herley, C., & Van Oorschot, P. C. (2014). An administrator's guide to internet password research. *28th Large Installation System Administration Conference (LISA14)*, 44–61.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Furnell, S. (2007). An assessment of website password practices. *Computers & Security*, *26*(7), 445–451. https://doi.org/10.1016/j.cose.2007.09.001

Furnell, S. (2022). Assessing website password practices – Unchanged after fifteen years? *Computers & Security*, *120*, 102790. https://doi.org/10.1016/j.cose.2022.102790

Furnell, S., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security*, *75*, 1–9.

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. *Proceedings of the Second Symposium on Usable Privacy and Security*, 44–55.

Gebauer, J., Kline, D. M., & He, L. (2011). Password Security Risk versus Effort: An Exploratory Study on User-Perceived Risk and the Intention to Use Online Applications. *Journal of Information Systems Applied Research*, *4*(2), 52.

Google. (n.d.). Authentication | Google Developers. Retrieved 27 January 2023, from https://developers.google.com/identity/authentication

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256–267. https://doi.org/10.1016/j.intcom.2011.03.007

Grimes, M., & Marquardson, J. (2019). Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems*, *119*, 23–34. https://doi.org/10.1016/j.dss.2019.02.010

Groves, R. M., Presser, S., & Dipko, S. (2004). The Role of Topic Interest in Survey Participation Decisions. *Public Opinion Quarterly*, *68*(1), 2–31. https://doi.org/10.1093/poq/nfh002

Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, *30*(4), 208–220. https://doi.org/10.1016/j.cose.2010.12.001

Guo, Y., Zhang, Z., & Guo, Y. (2019). Optiwords: A new password policy for creating memorable and strong passwords. *Computers & Security*, *85*, 423–435. https://doi.org/10.1016/j.cose.2019.05.015

Guo, Z., Cho, J.-H., Chen, I.-R., Sengupta, S., Hong, M., & Mitra, T. (2021). Online Social Deception and Its Countermeasures: A Survey. *IEEE Access*, *9*, 1770–1806. https://doi.org/10.1109/ACCESS.2020.3047337

Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

Hallamaa, T. (2022, April 5). Analyysi: Ukrainan sota toi kyberaseet rintamalle, jolla ei ole rajoja – nyt verkkohyökkäyksiin varaudutaan kaikkialla, myös Suomessa. *Yle*. Retrieved from https://yle.fi/uutiset/3-12386997

Hämäläinen, V.-P. (2021, January 27). Ehkä jopa 32 000 Vastaamon potilaan tiedot ilmestyivät viime yönä Tor-verkkoon – poliisi: 'Emme tiedä, monenko käsissä tietokanta on'. *Yle*. Retrieved from https://yle.fi/uutiset/3-11757676

Hämäläinen, V.-P., & Rummukainen, A. (2020, October 31). Yksi heistä on kiristäjä. *Yle*. Retrieved from https://yle.fi/uutiset/3-11616210

Hanus, B., & Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842

Heartfield, R., & Loukas, G. (2015). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys*, *48*(3), 37:1-37:39. https://doi.org/10.1145/2835375

Helpinen, V. (2022, September 14). Lukuisilta S-pankin tileiltä on viety rahaa laittomasti – Poliisi: Maksuvälinepetoksia ainakin 53, tietomurtoja noin 150. *Yle*. Retrieved from https://yle.fi/a/3-12623785

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61–84. https://doi.org/10.1111/j.1365-2575.2012.00420.x

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Holt, L. (2011). Increasing real-world security of user IDs and passwords. *Proceedings of the 2011 Information Security Curriculum Development*

Conference, 34–41. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2047456.2047461

Holt, T., & Bossler, A. (2015). : *Theory and prevention of technology-enabled offenses*. London: Routledge. https://doi.org/10.4324/9781315775944

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically Understanding the Cyber Attack Business: A Survey. *ACM Computing Surveys*, *51*(4), 70:1-70:36. https://doi.org/10.1145/3199674

International Telecommunication Union. (2008). *Recommendation ITU-T X.1205: Overview of cybersecurity*. Telecommunication Standardization Sector of ITU. Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549-A4. https://doi.org/10.2307/25750691

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, *39*(1), 113–134.

Jones, S. L., Collins, E. I. M., Levordashka, A., Muir, K., & Joinson, A. (2019). What is 'Cyber Security'? Differential Language of Cyber Security Across the Lifespan. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–6. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3290607.3312786

Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers & Security*, *127*, 103089. https://doi.org/10.1016/j.cose.2022.103089

Khan, S. H., Ali Akbar, M., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. *Pattern Recognition*, *48*(2), 458–472. https://doi.org/10.1016/j.patcog.2014.08.024

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, *8*, 125140–125148. https://doi.org/10.1109/ACCESS.2020.3007867

Lee, M. K. O., & Turban, E. (2001). A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce*, *6*(1), 75–91. https://doi.org/10.1080/10864415.2001.11044227

Leponen, M. (2022, February 11). Uusi, huolestuttava ilmiö—Rikolliset kohdistavat Vastaamo-tietovuodon uhreihin raukkamaisia rikoksia. Retrieved 26 April 2022, from https://poliisi.fi/blogi/-/blogs/uusi-huolestuttava-ilmio-rikolliset-kohdistavat-vastaamo-tietovuodon-uhreihin-raukkamaisia-rikoksia

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, *126*, 106979. https://doi.org/10.1016/j.chb.2021.106979

LLC Verizon. (2022). *2022 Data Breach Investigations Report*. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

Loula, P. (2022, April 26). Noin 20 000 asiakkaan varaustiedot vuosivat kahdesta suomalaishotellista – poliisi aloitti tietomurtotutkinnan. *Helsingin Sanomat*. Retrieved from https://www.hs.fi/kotimaa/art-2000008774004.html

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Marky, K., Ragozin, K., Chernyshov, G., Matviienko, A., Schmitz, M., Mühlhäuser, M., … Kunze, K. (2022). "Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication. *ACM Transactions on Computer-Human Interaction*, *29*(5), 43:1-43:32. https://doi.org/10.1145/3503514

Mayer, P., Zou, Y., Schaub, F., & Aviv, A. J. (2021). 'Now I'm a bit angry:' Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. *30th USENIX Security Symposium, Vancouver, CDN, August 11-13, 2021*, 393. Retrieved from https://www.usenix.org/conference/usenixsecurity21/presentation/mayer

Mazurek, M. L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., … Ur, B. (2013). Measuring password guessability for an entire university. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 173–186. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2508859.2516726

McCrae, R. R. (1984). Situational determinants of coping responses: Loss, threat, and challenge. *Journal of Personality and Social Psychology*, *46*(4), 919–928. (1984-23131-001). https://doi.org/10.1037/0022-3514.46.4.919

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Mohsin, J. K., Han, L., Hammoudeh, M., & Hegarty, R. (2017). Two Factor Vs Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. *Proceedings of the International Conference on Future Networks and Distributed Systems*, 1–10. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3102304.3102343

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, *23*(4), 18. https://doi.org/10.1007/s11920-021-01228-w

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, *135*, 113323. https://doi.org/10.1016/j.dss.2020.113323

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines. *Communications of the Association for Information Systems*, *42*, 7. https://doi.org/10.17705/1CAIS.04207

Nabi, R. L., Roskos-Ewoldsen, D., & Dillman Carpentier, F. (2008). Subjective Knowledge and Fear Appeal Effectiveness: Implications for Message Design. *Health Communication*, *23*(2), 191–201. https://doi.org/10.1080/10410230701808327

Nelson, D., & Vu, K.-P. L. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior*, *26*(4), 705–715. https://doi.org/10.1016/j.chb.2010.01.007

Ng, K. C., Zhang, X., Thong, J. Y. L., & Tam, K. Y. (2021). Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective. *Journal of Management Information Systems*, *38*(3), 732–764. https://doi.org/10.1080/07421222.2021.1962601

NICCS. (2022, July 6). Glossary | NICCS. Retrieved 24 August 2022, from https://niccs.cisa.gov/cybersecurity-career-resources/glossary

Ogbanufe, O. (2023). Securing online accounts and assets: An examination of personal investments and protection motivation. *International Journal of*

Information Management, *68*, 102590. https://doi.org/10.1016/j.ijinfomgt.2022.102590

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, *91*(12), 2021–2040. https://doi.org/10.1109/JPROC.2003.819611

O'Gorman, L., Bagga, A., & Bentley, J. (2005). Query-directed passwords. *Computers & Security*, *24*(7), 546–560. https://doi.org/10.1016/j.cose.2005.06.006

Olson, K. E., O'Brien, M. A., Rogers, W. A., & Charness, N. (2011). Diffusion of Technology: Frequency of use for Younger and Older Adults. *Ageing International*, *36*(1), 123–145. https://doi.org/10.1007/s12126-010-9077-9

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Onaolapo, J., Mariconti, E., & Stringhini, G. (2016). What Happens After You Are Pwnd: Understanding the Use of Leaked Webmail Credentials in the Wild. *Proceedings of the 2016 Internet Measurement Conference*, 65–79. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2987443.2987475

Paajanen, O.-P., Keski-Heikkilä, A., & Halminen, L. (2022, April 8). Valtion verkkosivut joutuivat verkkohyökkäyksen kohteeksi – Ulkoministeriö tekee asiasta rikosilmoituksen. *Helsingin Sanomat*. Retrieved from https://www.hs.fi/kotimaa/art-2000008738855.html

Padallan, J. O. (2019). *Cyber Security*. Arcler Press.

Parmar, V., Sanghvi, H. A., Patel, R. H., & Pandya, A. S. (2022). A Comprehensive Study on Passwordless Authentication. *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 1266–1275. https://doi.org/10.1109/ICSCDS53736.2022.9760934

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, *7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Peisert, S., Talbot, E., & Kroeger, T. (2013). Principles of authentication. *Proceedings of the 2013 New Security Paradigms Workshop*, 47–56. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2535813.2535819

Punch, K. F. (2003). *Survey Research: The Basics*. London: Sage.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Riek, M., Böhme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273. https://doi.org/10.1109/TDSC.2015.2410795

Rochat, J., & Ragot, M. (2022). Adoption of Green IT Behaviours: A Perceived Knowledge Effect on Responsible Digital Practices? *Adjunct Publication of the 24th International Conference on Human-Computer Interaction with Mobile Devices and Services*, 1–6. https://doi.org/10.1145/3528575.3551438

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114.

Rui, Z., & Yan, Z. (2019). A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access*, *7*, 5994–6009. https://doi.org/10.1109/ACCESS.2018.2889996

Sabzevar, A. P., & Stavrou, A. (2008). Universal Multi-Factor Authentication Using Graphical Passwords. *2008 IEEE International Conference on Signal Image Technology and Internet Based Systems*, 625–632. https://doi.org/10.1109/SITIS.2008.92

Sanastokeskus TSK ry. (2018). *Kyberturvallisuuden sanasto (TSK 52)*. Retrieved from https://sanastokeskus.fi/tsk/fi/kyberturvallisuuden_sanasto_tsk_52-1125.html

Schneier, B. (2015). *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons.

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, *32*(2), 314–341. https://doi.org/10.1080/07421222.2015.1063315

Sharma, A., Belwal, R. C., Ojha, V., & Agarwal, G. (2010). Password based authentication: Philosophical survey. *2010 IEEE International Conference on Intelligent Computing and Intelligent Systems*, *3*, 619–622. https://doi.org/10.1109/ICICISYS.2010.5658405

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security*, *61*, 130–141.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1753326.1753383

Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Computers & Security*, *88*, Article 101617. https://doi.org/10.1016/j.cose.2019.101617

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

Song, J., Wang, D., Yun, Z., & Han, X. (2019). Alphapwd: A Password Generation Strategy Based on Mnemonic Shape. *IEEE Access*, *7*, 119052–119059. https://doi.org/10.1109/ACCESS.2019.2937030

Stobert, E., & Biddle, R. (2018). The Password Life Cycle. *ACM Transactions on Privacy and Security*, *21*(3), 13:1-13:32. https://doi.org/10.1145/3183341

Sturman, D., Valenzuela, C., Plate, O., Tanvir, T., Auton, J. C., Bayl-Smith, P., & Wiggins, M. W. (2023). The role of cue utilization in the detection of phishing emails. *Applied Ergonomics*, *106*, 103887. https://doi.org/10.1016/j.apergo.2022.103887

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., … Bursztein, E. (2017). Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1421–1434. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3133956.3134067

Tilastokeskus. (2021). *Sukupuolten tasa-arvo Suomessa 2021*. Helsinki. Retrieved from https://www.doria.fi/handle/10024/184395

Traficom. (2022, September 12). Kyberympäristön uhkataso on noussut—Aktiviteetti Suomeakin kohtaan on lisääntynyt. Retrieved 21 October 2022, from https://www.traficom.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

Turvallisuuskomitea. (2019). *Finland´s Cyber Security Strategy 2019*. Retrieved from https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/

University of Jyväskylä. (2020, July 13). Information technology services—Digital Services. Retrieved 3 November 2023, from https://www.jyu.fi/digipalvelut/en/guides/for-new-student/it-services

University of Jyväskylä. (2022a, June 3). Multifactor authentication in University of Jyväskylä—Digital Services. Retrieved 8 February 2023, from https://www.jyu.fi/digipalvelut/en/guides/multifactor-authentication-in-university-of-jyvaskyla

University of Jyväskylä. (2022b, November 18). Instructions for students on the deployment of Microsoft multi-factor authentication—University of Jyväskylä. Retrieved 2 February 2023, from https://www.jyu.fi/en/current/archive/2022/11/instructions-for-students-on-the-deployment-of-microsoft-multi-factor-authentication

University of Jyväskylä. (2023a, February 6). Microsoft Multi-Factor Authentication becomes obligatory in spring 2023 – Please enable it as soon as possible! —University of Jyväskylä. Retrieved 9 March 2023, from https://www.jyu.fi/en/current/archive/2023/02/microsoft-multi-factor-authentication-becomes-obligatory-in-spring-2023-2013-please-enable-it-as-soon-as-possible

University of Jyväskylä. (2023b, February 6). Microsoftin monivaiheinen tunnistautuminen muuttuu pakolliseksi keväällä 2023 – Ota käyttöön pikimmiten! —Jyväskylän yliopisto. Retrieved 16 February 2023, from https://www.jyu.fi/fi/ajankohtaista/arkisto/2023/02/microsoftin-monivaiheinen-tunnistautuminen-muuttuu-pakolliseksi-kevaalla-2023-2013-ota-kayttoon-pikimmiten

University of Jyväskylä. (2023c, February 9). Jyväskylän yliopiston tietojärjestelmien käyttösäännöstö—Digipalvelut. Retrieved 3 November 2023, from https://www.jyu.fi/digipalvelut/fi/ohjeet/tietotekniikan-kayton-ja-yllapidon-saannot/jyvaskylan-yliopiston-tietojarjestelmien-kayttosaannosto-1

University of Jyväskylä. (2023d, August 8). Important web services for student—Digital Services. Retrieved 3 November 2023, from https://www.jyu.fi/digipalvelut/en/guides/for-new-student/web-services

University of Jyväskylä. (2023e, September 19). Office 365—M365—Digipalvelut. Retrieved 3 November 2023, from https://www.jyu.fi/digipalvelut/fi/ohjeet/office-365-ohjeet/o365

University of Jyväskylä. (2023f, October 17). Info for a new student—Digital Services. Retrieved 3 November 2023, from https://www.jyu.fi/digipalvelut/en/guides/for-new-student/info-package-for-a-new-student

University of Jyväskylä. (n.d.-a). Faculties, departments and independent institutes | University of Jyväskylä. Retrieved 7 November 2023, from https://www.jyu.fi/en/faculties-and-departments

University of Jyväskylä. (n.d.-b). Guides—Digital Services. Retrieved 3 November 2023, from https://www.jyu.fi/digipalvelut/en/guides

University of Jyväskylä. (n.d.-c). University—University of Jyväskylä. Retrieved 18 October 2023, from https://www.jyu.fi/en/university/university

Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., … Melicher, W. (2017). Design and Evaluation of a Data-Driven Password Meter. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 3775–3786. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3025453.3026050

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). Do Users' Perceptions of Password Security Match Reality? *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 3748–3760. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2858036.2858546

Vance, A., Eargle, D., Eggett, D., Straub, D. W., & Ouimet, K. (2022). Do Security Fear Appeals Work When They Interrupt Tasks? A Multi-Method Examination of Password Strength. *MIS Quarterly*, *46*(3), 1721–1737. https://doi.org/10.25300/MISQ/2022/15511

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, *94*, 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

Vilkka, H. (2007). *Tutki ja mittaa: Määrällisen tutkimuksen perusteet*. Helsinki: Tammi.

Vishwanath, A. (2015). Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication*, *20*(1), 83–98. https://doi.org/10.1111/jcc4.12100

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

von Zezschwitz, E., De Luca, A., & Hussmann, H. (2014). Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance. *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, 461–470. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2639189.2639218

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L. B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, *65*(8), 744–757.

Wahab, A. A., Hou, D., & Schuckers, S. (2023). A User Study of Keystroke Dynamics as Second Factor in Web MFA. *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, 61–72. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3577923.3583642

Wang, C., Wang, D., Xu, G., & Guo, Y. (2017). A lightweight password-based authentication protocol using smart card. *International Journal of Communication Systems*, *30*(16), e3336. https://doi.org/10.1002/dac.3336

Wang, D., Zhang, X., Zhang, Z., & Wang, P. (2020). Understanding security failures of multi-factor authentication schemes for multi-server environments. *Computers & Security*, *88*, 101619. https://doi.org/10.1016/j.cose.2019.101619

Wang, D., Zhang, Z., Wang, P., Yan, J., & Huang, X. (2016). Targeted Online Password Guessing: An Underestimated Threat. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1242–1254. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2976749.2978339

Wang, J., Li, Y., & Rao, H. R. (2017). Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences. *Information Systems Research*, *28*(2), 378–396. https://doi.org/10.1287/isre.2016.0680

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, *21*(1), 105–125. https://doi.org/10.1016/j.chb.2003.11.008

West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2009). The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions. In *Social and Human Elements of Information Security: Emerging Trends and Countermeasures* (pp. 43–60). IGI Global. https://doi.org/10.4018/978-1-60566-036-3.ch004

Wheeler, E. (2011). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Elsevier Science & Technology Books.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7. https://doi.org/10.1089/cyber.2014.0179

Woods, D. W., & Walter, L. (2022). Reviewing Estimates of Cybercrime Victimisation and Cyber Risk Likelihood. *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 150–162. https://doi.org/10.1109/EuroSPW55150.2022.00021

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*, *111*, 36–48. https://doi.org/10.1016/j.ijhcs.2017.11.002

Woods, N., & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies*, *128*, 61–71. https://doi.org/10.1016/j.ijhcs.2019.02.003

Xie, Y., Siponen, M., Moody, G., & Zheng, X. (2022). Discovering the interplay between defensive avoidance and continued use intention of anti-malware software among experienced home users: A moderated mediation model. *Information & Management*, *59*(2), 103586. https://doi.org/10.1016/j.im.2021.103586

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741–759. https://doi.org/10.1007/s10207-019-00429-y

Zhang, L., & McDowell, W. C. (2009). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. *Journal of Internet Commerce*, *8*(3–4), 180–197. https://doi.org/10.1080/15332860903467508

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, *133*, 26–44. https://doi.org/10.1016/j.ijhcs.2019.08.006

APPENDIX 1: PILOT SURVEY ITEMS

Construct	Item	Question	Source / Adapted from
Perceived Knowledge	PercKnow1	I feel adequately informed about the risks of the internet.	De Kimpe et al., 2022
	PercKnow2	I feel adequately informed about how to avoid the risks of the internet.	
Internet Trust	Trust1	I am optimistic about the safety of the internet.	De Kimpe et al., 2022
	Trust2	I have every confidence that the internet is safe.	
	Trust3	I am satisfied with the safety of the internet.	
Past Data Breach Experience	Experience1	I was a victim of a data breach. *Original question:* *I was a victim of an invasion of privacy.*	Mousavi et al., 2020
	Experience2	My information has been misused on the internet.	
	Experience3	My information has been used by an unauthorized party before.	
Perceived Severity	PercSev1	If my university user account were hacked, it would affect me severely. *Original question: If my email were hacked, it would affect me severely.*	Ng et al., 2021
	PercSev2	If my university user account were hacked, it would affect me seriously. *Original question: If my email were hacked, it would affect me seriously.*	
	PercSev3	If my university user account were hacked, it would affect me significantly. *Original question: If my email were hacked, it would affect me significantly.*	
Perceived Vulnerability	PercVuln1	It is possible that I will be a victim of a data breach through my university account being hacked. *Original question: It is possible that I will be a victim of cybercrime.*	De Kimpe et al., 2022
	PercVuln2	It is likely that I will be a victim of a data breach through my university account being hacked. *Original question: It is likely that I will be a victim of cybercrime.*	
	PercVuln3	There is a great risk that I'll be a victim of a data breach through my university account being hacked. *Original question: There is a great risk that I'll be a victim of cybercrime.*	

Fear	Fear1	I am worried about my university user account being hacked. *Original question: I am worried about my email being hacked.*	Ng et al., 2021
	Fear2	I am frightened about my university user account being hacked. *Original question: I am frightened about my email being hacked.*	
	Fear3	I am anxious about my university user account being hacked. *Original question: I am anxious about my email being hacked.*	
	Fear4	I am scared about my university user account being hacked. *Original question: I am scared about my email being hacked.*	
Multifactor Authentication Response Efficacy	MfaRespEff1	Multifactor authentication works for protection. *Original question: Anti-spyware software works for protection.*	Johnston & Warkentin, 2010
	MfaRespEff2	Multifactor authentication is effective for protection. *Original question: Anti-spyware software is effective for protection.*	
	MfaRespEff3	When using multifactor authentication, my university user account is more likely to be protected. *Original question: When using anti-spyware software, a computer is more likely to be protected.*	
Multifactor Authentication Self-Efficacy	MfaSelfEff1	I believe I could easily activate multi-factor authentication to prevent account hacking.	Ogbanufe, 2023
	MfaSelfEff2	It would be easy for me to use a multi-factor authentication to avoid account hacking.	
	MfaSelfEff3	I believe I could use multi-factor authentication to prevent account hacking.	
	MfaSelfEff4	I am capable of successfully using multi-factor authentication to avoid account hacking.	
Multifactor Authentication Response Costs	MfaRespCost1	Using multi-factor authentication on my university user account would require considerable effort. *Original question: Using multi-factor authentication on my online accounts would require considerable effort.*	
	MfaRespCost2	Taking the time to use multi-factor authentication on my university user account would take too much time. *Original question: Taking the time to use multi-*	

		factor authentication on my online accounts would take too much time.	
	MfaRespCost3	Using multi-factor authentication would be too much work.	
Multifactor Authentication Behavioral Intention	MfaBeInt1	I intend to use multifactor authentication for my university user account in the next month. *Original question: I intend to use anti-spyware software in the next 3 months.*	Johnston & Warkentin, 2010
	MfaBeInt2	I predict I will use multifactor authentication for my university user account in the next month. *Original question: I predict I will use anti-spyware software in the next 3 months.*	
	MfaBeInt3	I plan to use multifactor authentication for my university user account in the next month. *Original question: I plan to use anti-spyware software in the next 3 months.*	
Password Response Efficacy	PwRespEff1	I can protect my university user account better if I use strong passwords. *Original question: I can protect my online accounts better if I use strong passwords.*	Zhang & McDowell, 2009
	PwRespEff2	I can protect my university user account better if I update my passwords often. *Original question: I can protect my online accounts better if I update my passwords often,*	
	PwRespEff3	I can protect my university user account better if I use unique passwords for each online account. *Original question: I can protect my online accounts better if I use unique passwords for each online accounts.*	
Password Self-Efficacy	PwSelfEff1	I would be able to create a strong password that is difficult to hack if I had instructions on how to create a strong password.	Mwagwabi et al., 2018
	PwSelfEff2	I would be able to create a strong password that is difficult to hack if I had step-by-step instructions on how to memorize a strong password.	
	PwSelfEff3	I would be able to create a strong password that is difficult to hack if I had a lot of time to create a strong password.	
	PwSelfEff4	I would be able to create a strong password that is difficult to hack if I had used strong passwords before.	
Password Response Costs	PwRespCost1	If I use strong passwords, they will be difficult for me to remember.	Zhang & McDowell, 2009
	PwRespCost2	If I update my passwords often, they will be difficult for me to remember.	
	PwRespCost3	If I use unique password on each account, they will be difficult for me to remember.	

Password Behavioral Intention	PwBeInt1	I intend to use a strong password for my university user account in the next month. *Original question: I intend to use anti-spyware software in the next 3 months.*	Johnston & Warkentin, 2010
	PwBeInt2	I predict I will use a strong password for my university user account in the next month. *Original question: I predict I will use anti-spyware software in the next 3 months.*	
	PwBeInt3	I plan to use a strong password for my university user account in the next month. *Original question: I plan to use anti-spyware software in the next 3 months.*	
Defensive Avoidance	DefAvoi1	I try not to let the thought of my university user account being hacked enter my mind. *Original question: I try not to let the thought of spyware enter my mind.*	Chenoweth et al., 2019
	DefAvoi2	I try not to think about the possibility of my university user account being hacked. *Original question: I try not to think about the possibility of my computer being infected by spyware.*	
	DefAvoi3	I try to ignore the possibility of my university user account being hacked. *Original question: I try to ignore the possibility of being infected by spyware.*	

APPENDIX 2: MAIN SURVEY ITEMS

Construct	Item	Question	Source / Adapted from
Perceived Knowledge	PercKnow1	I feel adequately informed about the risks of the internet.	De Kimpe et al., 2022
	PercKnow2	I feel adequately informed about how to avoid the risks of the internet.	
	PercKnow3	I have an adequate amount of knowledge about the risks of the internet. *Original question:* *I have a lot of knowledge about Green IT.*	Rochat & Ragot, 2022
Internet Trust	Trust1	I am optimistic about the safety of the internet.	De Kimpe et al., 2022
	Trust2	I have every confidence that the internet is safe.	
	Trust3	I am satisfied with the safety of the internet.	
Past Data Breach Experience	Experience1	I was a victim of a data breach. *Original question:* *I was a victim of an invasion of privacy.*	Mousavi et al., 2020
	Experience2	My information has been misused on the internet.	
	Experience3	My information has been used by an unauthorized party before.	
Perceived Severity	PercSev1	If my university user account were hacked, it would affect me severely. *Original question: If my email were hacked, it would affect me severely.*	Ng et al., 2021
	PercSev2	If my university user account were hacked, it would affect me seriously. *Original question: If my email were hacked, it would affect me seriously.*	
	PercSev3	If my university user account were hacked, it would affect me significantly. *Original question: If my email were hacked, it would affect me significantly.*	
Perceived Vulnerability	PercVuln1	It is possible that I will be a victim of a data breach through my university account being hacked. *Original question: It is possible that I will be a victim of cybercrime.*	De Kimpe et al., 2022
	PercVuln2	It is likely that I will be a victim of a data breach through my university account being hacked. *Original question: It is likely that I will be a victim of cybercrime.*	
	PercVuln3	There is a great risk that I'll be a victim of a data breach through my university account	

		being hacked. *Original question: There is a great risk that I'll be a victim of cybercrime.*	
Fear	Fear1	I am worried about my university user account being hacked. *Original question: I am worried about my email being hacked.*	Ng et al., 2021
	Fear2	I am frightened about my university user account being hacked. *Original question: I am frightened about my email being hacked.*	
	Fear3	I am anxious about my university user account being hacked. *Original question: I am anxious about my email being hacked.*	
	Fear4	I am scared about my university user account being hacked. *Original question: I am scared about my email being hacked.*	
Multifactor Authentication Response Efficacy	MfaRespEff1	Multifactor authentication works for protection. *Original question: Anti-spyware software works for protection.*	Johnston & Warkentin, 2010
	MfaRespEff2	Multifactor authentication is effective for protection. *Original question: Anti-spyware software is effective for protection.*	
	MfaRespEff3	When using multifactor authentication, my university user account is more likely to be protected. *Original question: When using anti-spyware software, a computer is more likely to be protected.*	
Multifactor Authentication Self-Efficacy	MfaSelfEff1	I believe I could easily activate multi-factor authentication to prevent account hacking.	Ogbanufe, 2023
	MfaSelfEff2	It would be easy for me to use a multi-factor authentication to avoid account hacking.	
	MfaSelfEff3	I believe I could use multi-factor authentication to prevent account hacking.	
	MfaSelfEff4	I am capable of successfully using multi-factor authentication to avoid account hacking.	
Multifactor Authentication Response Costs	MfaRespCost1	Using multi-factor authentication on my university user account would require considerable effort. *Original question: Using multi-factor authentication on my online accounts would require considerable effort.*	
	MfaRespCost2	Taking the time to use multi-factor authentication on my university user account would take too much time.	

		Original question: Taking the time to use multi-factor authentication on my online accounts would take too much time.	
	MfaRespCost3	Using multi-factor authentication would be too much work.	
Multifactor Authentication Behavioral Intention	MfaBeInt1	I intend to use multifactor authentication for my university user account in the next 4 weeks. *Original question: I intend to use anti-spyware software in the next 3 months.*	Johnston & Warkentin, 2010
	MfaBeInt2	I predict I will use multifactor authentication for my university user account in the next 4 weeks. *Original question: I predict I will use anti-spyware software in the next 3 months.*	
	MfaBeInt3	I plan to use multifactor authentication for my university user account in the next 4 weeks. *Original question: I plan to use anti-spyware software in the next 3 months.*	
Password Response Efficacy	PwRespEff1	I can protect my university user account better if I use strong passwords. *Original question: I can protect my online accounts better if I use strong passwords.*	Zhang & McDowell, 2009
	PwRespEff2	I can protect my university user account better if I update my passwords often. *Original question: I can protect my online accounts better if I update my passwords often,*	
	PwRespEff3	I can protect my university user account better if I use unique passwords for each online account. *Original question: I can protect my online accounts better if I use unique passwords for each online accounts.*	
	PwRespEff4	I can protect my university user account better if I do not reuse passwords.	Original question
Password Self-Efficacy	PwSelfEff1	I would be able to create a strong password that is difficult to hack if I had instructions on how to create a strong password.	Mwagwabi et al., 2018
	PwSelfEff2	I would be able to create a strong password that is difficult to hack if I had step-by-step instructions on how to memorize a strong password.	
	PwSelfEff3	I would be able to create a strong password that is difficult to hack if I had a lot of time to create a strong password.	
	PwSelfEff4	I would be able to create a strong password that is difficult to hack if I had used strong passwords before.	
Password Response Costs	PwRespCost1	If I use strong passwords, they will be difficult for me to remember.	Zhang & McDowell, 2009
	PwRespCost2	If I update my passwords often, they will be difficult for me to remember.	
	PwRespCost3	If I use unique password on each account, they	

		will be difficult for me to remember.	
Password Behavioral Intention	PwBeInt1	I intend to use a strong password for my university user account in the next 4 weeks. *Original question: I intend to use anti-spyware software in the next 3 months.*	Johnston & Warkentin, 2010
	PwBeInt2	I predict I will use a strong password for my university user account in the next 4 weeks. *Original question: I predict I will use anti-spyware software in the next 3 months.*	
	PwBeInt3	I plan to use a strong password for my university user account in the next 4 weeks. *Original question: I plan to use anti-spyware software in the next 3 months.*	
Defensive Avoidance	DefAvoi1	I try not to let the thought of my university user account being hacked enter my mind. *Original question: I try not to let the thought of spyware enter my mind.*	Chenoweth et al., 2019
	DefAvoi2	I try not to think about the possibility of my university user account being hacked. *Original question: I try not to think about the possibility of my computer being infected by spyware.*	
	DefAvoi3	I try to ignore the thought of my university user account being hacked. *Original question: I try to ignore the possibility of being infected by spyware.*	