Master Degree Project

DO YOU FEAR YOUR PHONE?

Jonathan Haugen Ganander
b20jonga@student.his.se

Supervisor: Ali Padyab
Examiner: Rose-Mharie Åhlfeldt

Date of examination: 2022-06-23

Course code: IT777A

Master Degree Project (120 ECTS) in Informatics
with a specialization in
Privacy, Information and Cyber Security
30 ECTS
Spring term 2022

Acknowledgments

For all the guidance through this project, I would like to thank my supervisor, Ali. For the insightful comments, I would like to thank my examiner Rose-Mharie. Lastly, I would like to thank all family and friends who intentionally or unintentionally have helped me stay on track and finish this project.

ABSTRACT

Digital Natives are described as a generation who possess a different relation to information technology, including mobile phones. Mobile phones have quickly gone from strictly communication devices to rather sophisticated mobile computers. Because of an increase in capabilities, there is a need to ensure control over the mobile phone environment. One strategy that can be implemented to control the mobile phone environment is to amplify the severity and vulnerability of threats that can target mobile phones by introducing fear appeals. This study aimed to investigate how digital natives experienced fear in relation to their phones, exercising the idea of how well fear appeals would work in this context and if other aspects impact the digital native's security behavior. This was done by conducting semi-structured interviews with digital natives and analyzing the answers against the aspects of the protection motivation theory model. It was concluded that fear did not influence digital natives but rather other aspects, such as the convenience of use.

Table of Contents

1 Introduction

In 2001 Prensky coined the term “Digital Natives” for a new generation of people brought up in a digital context and with a different relation to digital tools compared to previous generations. Spanning people born in 1980 and forward, this generation is currently a large part of the workforce and will continue to grow when previous generations are heading for retirement. Individuals in this generation are likely to express narcissistic and individualistic traits which affect their view on risk-taking, seeking out personal benefits while blaming situations that goes wrong on an external party (Twenge & Campbell, 2008; Weeger et al., 2020). A clear example of this is provided by Weeger et al. (2020), where digital natives are found to place a large value on the benefits of participating in a *bring your own device* (BYOD) program while ignoring the risks that can be attributed to their behavior. For the digital native, risks that target the individual directly have a higher impact on their decision making while risks that do not pose an explicit threat against the individual are less likely to have an impact on the decision-making process. Furthermore, the digital natives' view on risks influences the decision to use privately owned digital devices in an organizational context or not by not being concerned with risks that can impact the organization while risks that do affect the digital native directly are of concern (Weeger et al., 2020).

Mobile digital devices have become an integrated part of modern human life. One source even claims that there are currently 7.1 billion mobile users in the world (Statista, 2021a) further highlighting the widespread usage of mobile phones. In Sweden, the number of private mobile subscriptions is just over 9,5 million, highlighting the widespread of privately owned devices accessible by individuals (Statista, 2021b). The possibility to use private devices is realized by the declining cost of IT technologies and digital devices, changing the digital environment from being utilized in a primarily professional context provided by organizations to a phenomenon that more and more people have access to in their private life (Jarrahi et al., 2017). This change has forced organizations to change their strategy regarding IT and not only rely on the availability aspect of digital tools. There are different ways of controlling which devices can be used in an organizational context, ranging from the strict *use what you are told* (UWYT) to the uncontrolled *bring your own device* (BYOD) which has various impacts when implemented (Brodin, 2016). Similar to the BYOD approach is the *choose your own device* (CYOD) strategy, where the main difference is that organizations have better control over the device when CYOD is implemented though this will include the cost of the devices. What is important to know for both strategies is that the user still needs to have a high degree of awareness and that information belonging to the organization can be stored externally on devices manly accessible to the individual that uses or own the device. Another point that is important to raise according to Weeger et al. (2020) is that the privately-owned devices will be used by digital natives either by introducing a BYOD program or by having uncontrollable devices within the confines of a company, known as Shadow IT.

In information security research there has been a research stream directed toward the applicability of fear appeals to affect individuals to comply with policies utilized by organizations (Boss et al., 2015; Crossler et al., 2013; Johnston

et al., 2015; Johnston & Warkentin, 2010). The usage of fear appeals has not only been seen in research but has been applied in software and organizations utilize them as well to influence individuals' information security behavior (Dupuis & Renaud, 2021).

Fear appeals can be used to influence individuals' behaviors when there is a clear "right way" to act when facing a threat (Floyd et al., 2000). People may still choose maladaptive responses (i.e., not choosing the right way to act) as there can be rewards to the individual. These "right" and "wrong" ways to act are according to the author or beneficiary of the fear appeals. Fear appeals have been included in different theories, where protection motivation theory (PMT) have been applied to a variety of field including information security (Johnston et al., 2015). Furthermore, Johnston et al. (2015) argue that all of the constructs available in the PMT model should be used and tested in the field of information security before other constructs not originating from the PMT model are added.

1.1 Problem Description

Digital natives are a part of the workforce that is continuously growing, and some parts of this demographic have been studied in relation to using partially or fully private devices in an organizational context (Jarrahi et al., 2017; Kerr & Koch, 2014; Weeger et al., 2020). Previous literature shows that digital natives show a lower interest in acting securely for the sake of the organization but are still concerned with threats that can affect them directly (Weeger et al., 2020). At the same time, security professionals' perceptions of digital natives' behavior have been recorded to mismatch with what behaviors digital natives are displaying, which could have implications for how security is handled (Gkioulos, Wangen, & Katsikas, 2017). Combined with the fact that there are concerns raised with different approaches to handling strategies for mobile devices (Brodin, 2016; Siddiquie et al., 2020) there is an indication that policies and regulations are unable to successfully influence when applied to digital natives. Although it is possible to increase user satisfaction and have a more secure IT environment by implementing CYOD for example, the organization is still dependent on choices by their employees regarding which device is used in which situation. An implementation of a strategy does not automatically ensure that employees comply (Brodin, 2016), and the individualistic traits of the digital native could be a further concern regarding compliance.

Yusif & Hafeez-Baig (2021) apply *protective motivated theory* (PMT) and compliance theory to higher education institutions (HEI) as they include generational differences characterized by digital natives, arguing that these two theories are the key to achieving cyber security compliance. This is, however, only applied to HEIs. The effectiveness of the current utilization of fear appeals in information security has previously been criticized by scholars (Boss et al., 2015; Johnston et al., 2015). Boss et al. (2015) argue that previous studies analyzing fear appeals in information security do not utilize the full nomology of PMT (i.e. all original constructs in PMT) before adding additional constructs. Examples of such models are *fear appeals model* (FAM) and *technology threat avoidance theory* (TTAT). According to Boss et al. (2015) these deriving models risk ending up weaker than the PMT model, both theoretically and empirically as they have not been

properly tested. PMT, on the other hand, is a well-established model. Boss et al. (2015) argue that models that derive from PMT need to be proven to be stronger in direct comparison to PMT to be a valid extension. Johnston et al. (2015) argue that fear appeals are rhetorically misconstructed and do not consider that there is a difference between threats targeting the individual and threats targeting an organization.

This study falls into the field of behavioral information security, a field that Crossler et al. (2013) claim is lacking in some prominent areas. Even though the technical aspect of information security is of uttermost importance, individuals' behavior concerning information assets needs to be expanded on. Fear appeals utilization to change individuals' security compliance behavior has previously been studied (Ifinedo, 2012; Johnston et al., 2015; Johnston & Warkentin, 2010; Vance et al., 2012), but there are still questions about how individual characteristics, such as personality types or perceptional readiness, affect the susceptibility to fear in a compliance context (Crossler et al., 2013). The current research stream into behavioral information security concerning fear appeals mostly utilizes surveys or lab experiments as a research methodology. Crossler et al. (2013), argue that a more varied use of methodologies could help to understand the effect fear appeals have on individuals in an information security context.

The problem that is going to be addressed in this thesis is thus the lack of understanding of digital natives' motives for complying or not complying with security policies regarding private devices. To what extent fear appeals can be used as a motivator, in this case, will be further studied.

1.2 Research Aim

As mobile phones today can be utilized for advanced tasks and hold a high amount of data of both professional and private character, it is important to control these devices to ensure that the information stays safe. Fear appeals have been proposed to help organizations boost compliance by enhancing the severity and vulnerability of a threat (Boss et al., 2015; Johnston et al., 2015; Johnston & Warkentin, 2010). At the same time, the two main constructs that are meant to be affected by a fear appeal (i.e. threat severity and threat vulnerability) have been recognized to not have an as strong impact on digital natives as previous generations (Li et al., 2022; Weeger et al., 2020).

There is a conflict between the difference in traits between digital natives and individuals not included in this generation and the problems that can arise from having private devices within the confines of a company. This work will thus aim to study why digital natives use or don't use privately owned devices for professional tasks. The specific aspect that will be investigated is to what extent fear appeals are effective for utilization to change digital natives' behavior regarding using private mobile phones. Thus, the research questions formulated for this study are:

1. How does fear affect digital natives in complying with policies regarding mobile devices?

2. In what way do the different aspects of PMT affect digital natives' usage of mobile phones?

To answer the questions presented above semi-structured interviews will be conducted with digital natives. The questions in the interviews will be based on the constructs in PMT. The semi-structured approach was applied to follow up and capture concepts that materialized during the interview and further understand the reasoning from the perspective of the respondents.

This work is outlined as follows. In chapter two an introduction to the main concepts is given and an overview of the previous research that has been conducted in the area. Chapter three presents the philosophy behind the research together with the method applied to study this area. Results are presented in chapter four followed by a discussion of the results in chapter five. A conclusion is presented in chapter six.

2 Background

This chapter is divided into two different subchapters. First, a review of the three main concepts of digital natives, mobile device strategies, and fear appeals are presented. Here the concepts are described and give a partially originating insight into where the concepts are deriving from. In the second part, a background into what research has been done on these concepts in conjunction with each other is presented.

2.1 Concepts

This section is divided into three main concepts that are relevant to this study. The first part concerns the topic of digital natives. Here is an explanation of what a digital native entails and some of the recognized characteristics of this group. The second part gives an overview of what strategies for handling mobile devices organizations can utilize. A brief overview will also be given of what advantages and disadvantages each strategy provides. In the third section fear appeals will be conceptualized together with concrete examples of fear appeals that can be encountered. A brief overview of fear appeals implementation in information security literature will also be given. Lastly, an introduction to PMT will be given.

2.1.1 Digital Natives

The term digital native has been around since its first occurrence in 2001 and was meant to highlight a new generation that was brought up with high access to technology from an early age (Prensky, 2001). In contrast to its counterpart, the digital immigrant, the usage of digital tools was a natural occurrence in everyday life rather than being applied in a limited manner in exclusive circumstances (e.g., in certain work scenarios, specific parts of society, etc.). This has resulted in digital natives forming a different relationship with digital technology and thus handling it in another way than digital immigrants. Perensky (2001) describes the difference between digital natives and digital immigrants in the following way:

> But the most useful designation I have found for them is Digital Natives. Our students today are all “native speakers” of the digital language of computers, video games, and the Internet. So what does that make the rest of us? Those of us who were not born into the digital world but have, at some later point in our lives, become fascinated by and adopted many or most aspects of the new technology are actively seeking alternatives to the distribution of traditional journal articles through a limited number of publishing houses that control rights and are considered to be making exceedingly large profits through their control of the distribution of what is seen, traditionally, as public knowledge. (p.1 & 3)

The dividing factor between these two different groups is thus if the individual can be considered to be born into the digital world or not. This can be viewed as partially different from previous divisions of generations that are given more concrete dates for their definition. Some scholars see digital natives as equivalent to millennials or generation y (Hallikainen et al., 2019; Jarrahi et al., 2017; Jeong et al., 2016; Margaryan et al., 2011; Shirish et al., 2016; Weeger et al.,

2020). This matches Prenskys (2001) definition by including the first generation of digital natives from 1980 to 1996. The statement includes that this is the *first* generation of digital natives however and that the individuals that are born into the digital world are its native speakers. Another view of the digital native status is presented by Li et al. (2022). Here the argument is that individuals born after 1996 should be considered digital natives (Li et al., 2022). This correlates with the statement of individuals that are born into the digital world but are targeting people that are out of the range of Prenskys age definition. Another point that is important to highlight is that Prensky (2001) attributes all people born before 1980 to the digital immigrant status. Based on the definition of people born into the digital world (i.e. individuals born in 1980 or later) and the choice to grant all people born before 1980 digital immigrant status, this thesis will use the definition of digital natives to mean people born in 1980 and later.

Digital natives are faster to adopt new IT than previous generations and are interested to use technology for the potential benefits which can be connected to the early age at which they were exposed to similar technologies (Jarrahi et al., 2017). Individuals that are part of this generation do also go under the names Millennial, Generation Y, Google generation, etc. (Helsper & Eynon, 2010). The term "digital natives" and the claim that they have unified characteristics towards the usage of new technologies have been criticized (Bennett et al., 2008; Helsper & Eynon, 2010; Jones et al., 2010). That the digital native would have a radically different preference for learning than previous generations is questioned by Bennett et al. (2008), but not that technology is used by this group to a wide extent. Jones et al. (2010) highlight a difference between "digital natives" and "digital immigrants" usage of *information and communication technologies* (ICT) such as instant messaging and participation in online social networks but are also opposed to Prensky's (2001) claim about the need for different learning styles for digital natives and digital immigrants. Helsper and Eynon (2010) recognize that linear decline is present between age groups and their usage of ICT, the Internet, and self-efficacy, but are arguing that there are other prominent factors for determining if one is a digital native or not such as experience and how much internet is used. Connaway et al. (2011) claim that convenience in information search is an increasing factor for individuals, and is especially visible among millennials.

Twenge & Campbell (2008) provide an in-depth analysis of 1.4 million records of scales for measuring behavior, attitude, and personality of individuals ranging from 1930 to 2008. What they conclude is that there is a distinct change in behavior between millennials and previous generations. The millennial shows more self-esteem and narcissistic attributes. They are also likely to attribute the cause or control of situations or events to their environment, resulting in the millennials being likely to take individual responsibility and blame their surroundings if something goes wrong. A trait that is visible from this generation is their increased confidence in the usage of digital tools, which can result in negligence in security matters (Gkioulos, Wangen, Katsikas, et al., 2017). Although when security threats are apparent for the digital native, they seem to take a more forceful stance in terms of security.

The digital native is also premiering functionality tied to their needs rather than opting for security measures but can be persuaded to adopt a more secure approach when presented with solutions deemed usable. How well digital natives utilize digital tools and to what degree they understand the effect of their actions in a digital environment can be disputed (Till & Densmore, 2019). Furthermore, according to Till and Densmore (2019), the digital native's lack of capability in identifying security and privacy issues in a mobile environment is imminent. An example of misconception about malicious practices is presented in a study by Krašna & Bratina (2011) where almost half of the participating digital natives had a misconception about what phishing is and a quarter of the participants classified identity theft wrong. Jarrahi et al. (2017) do not share the same view of the digital native, however, describing them as tech-savvy individuals that have developed different skills and a different mindset towards technologies (e.g., sharing knowledge informally, privacy, socialization through technology, etc.) compared to previous generations.

Weeger et al. (2020) claim that the digital natives possess narcissistic and individualistic traits, making them prone to not care about the dangers posed towards their digital surroundings tied to their actions unless they are under threat. The narcissistic traits are characterized by high self-esteem which can result in overconfidence (Twenge & Campbell, 2008). Narcissists do also have a harder time getting along with others, caused by a lack of empathy and more difficulty with adopting the perspective of another individual. Furthermore, narcissists are likely to take more risks (ibid.). In an information security context, this can materialize in the form of malware or viruses entering the company network, damaging the company but not so much the individual (Weeger et al., 2020). The digital natives are also described to be proactive in their adoption of digital tools rather than passively accepting technology (Kerr & Koch, 2014). It is also observed that digital natives adopt technologies that fit them when they perceive that the tools provided by the organization do not meet their requirements. Adoption of alternative digital tools occurs when the digital native perceives that the tools provided by the organization do not fulfill the digital native's requirement. Security professionals have a mismatched perception of the security awareness displayed among digital natives contrary to the actual security awareness of digital natives, having an inaccurate prediction rate of how the digital natives behave (Gkioulos, Wangen, & Katsikas, 2017).

2.1.2 Mobile Device Strategies

There are three main ways to control devices within an organization; UWYT, CYOD, and BYOD (Brodin, 2016). The traditional approach to managing digital devices is to implement a UWYT strategy, where the organizations have full control over the devices, there is a list of explicitly approved devices, and the configuration is solely for work purposes. In the case of CYOD, the organization buys and owns the device, but the device is chosen by the employee, can be used to some extent for private purposes, and enables employees to work with more flexibility. The last approach for mobile devices is BYOD where the employee uses their device for work purposes, causing the organization to lose all control of the device. UWYT does enable a higher degree of control, but the benefits of higher flexibility and user satisfaction are lost when this strategy is utilized (Brodin, 2016). Another way to control mobile devices is to implement

mobile device management (MDM), which can be used by organizations to perform activities to increase the security of organizational IT infrastructure (e.g., enable VPN connectivity and conduct malware scans, etc.) (Samarathunge et al., 2018). Differentiating from MDM there is also the approach of Enterprise Mobility Management (EMM), which enables a higher level of control of the device (Siddiquie et al., 2020; Mearian, 2017). Siddiquie et al. (2020) do however report that there are vulnerabilities in one of these solutions "android for work" which is designed to make devices able to use both in a private and professional context by enabling a secure professional user profile. The benefits of utilizing CYOD and BYOD are similar, making the employee able to be more productive, more flexible, and increasing user satisfaction (Brodin, 2016). The concern for mixing up organizational and private information is present when both strategies are utilized but a further concern is present when BYOD is used, namely what happens with the information when an employee is no longer a part of an organization where the individual was using a private device for professional tasks. Security awareness is important with both strategies but is more critical when BYOD is utilized since the control is close to non-existent. BYOD can also be of concern when trying to integrate devices against the organization's infrastructure. According to Weeger et al. (2020) even though an organization does not allow BYOD practices there is still a risk that these devices will be used by employees and create a situation where shadow IT instead becomes a problem. Even though the devices are not accepted by the organization they can still introduce a threat. This is a problem pointed out by Brodin (2016) as well, where a respondent had been facing that kind of problem. With this said, even if CYOD is implemented there is a risk that individuals who have access to privately owned devices can perceive benefits with utilizing these devices in an organizational setting.

Traditional approaches to managing organizational IT may provide control and results in the short term, but also risk alienating applicants and to be a long-term demotivator for employees (Jarrahi et al., 2017). This becomes a more and more likely scenario as individuals become more accustomed to IS in their private life (Ostermann & Wiewiorra, 2017). Jarrahi et al. (2017) propose that managers recognize the shift in IT adaption in order to successfully adopt new inventions into the organizational IT environment. A recognized shift in it adoption could also leed to contempt employees.

2.1.3 Fear Appeals

Fear is described as a primary emotion in psychology, included in the emotions that can be first felt when encountered with stimuli (Warkentin et al., 2016). After the primary emotion response, a secondary response is further triggered, for example, anger, which then leads to a behavioral response.

Fear appeals are a message that is designed to persuade individuals to take a recommended action by manipulating the fear of a threat (Boss et al., 2015; Johnston & Warkentin, 2010). The components directly manipulated by the fear appeal are the perceived threat severity and threat vulnerability. This is to change an individual's behavior in choosing the right way to act according to the beneficiary of the fear appeal usage.

Fear appeals have been used to a large extent in health communication(Ruiter et al., 2014). It is believed to change individuals' motivation to adopt safer behaviors by displaying the devastating effects of certain risks. As larger campaigns like anti-smoking (see figure 1) and advocacy for using seatbelts. The usage of fear has also been adapted to other domains, including information security where the usage of fear appeals tries to affect individuals to comply with security policies(Boss et al., 2015; Johnston et al., 2015; Johnston & Warkentin, 2010; Jones et al., 2010; Warkentin et al., 2016). Furthermore, fear appeals have not only been used in literature but also in practical implementation to change behavior regarding information assets (see figure 2).

Figure 1. Fear appeal used in an anti-smoking campaign.

Fear appeal is described by Boss et al. (2015) to be the core component that needs to be manipulated to influence the behavior of users, which in information security literature often gets overlooked. Their study indicates that there is a large difference when comparing behavior intentions and behavior, where the large majority of information security research using PMT measures behavior intentions. To use fear appeals in a successful way Boss et al. (2015) argue that fear appeals need to be included in efforts spanning over a longer period, like campaigns and training. Furthermore, the maladaptive benefits and response cost should be minimized so maladaptive behavior is not appealing to the end-user. Johnston et al. (2015) claim that fear appeals are often misused in how their rhetorical composition is formulated by IS scholars and practitioners alike. Models including fear appeals often are used incorrectly, by omitting constructs, e.g. fear, or by introducing constructs that do not originally exist in the PMT model, e.g. social influence (ibid.). They claim that placing more emphasis on the threat against the individual can complement the threat to the information asset, forming a threat appeal that the individual perceives as more harmful. Threat appeals have been used in other theories related to information security, but Boss et al. (2015) strongly advise that the full nomology of PMT should be used and tested in an information security context before adding components that are not part of the PMT nomology.

Warkentin et al. (2016) find neurological evidence for a difference in brain activation of an individual when encountered with threat and threat responses related to IS security compared to natural statements. What is not noticed, however, is any indication that individuals experience any emotional reaction, including fear.

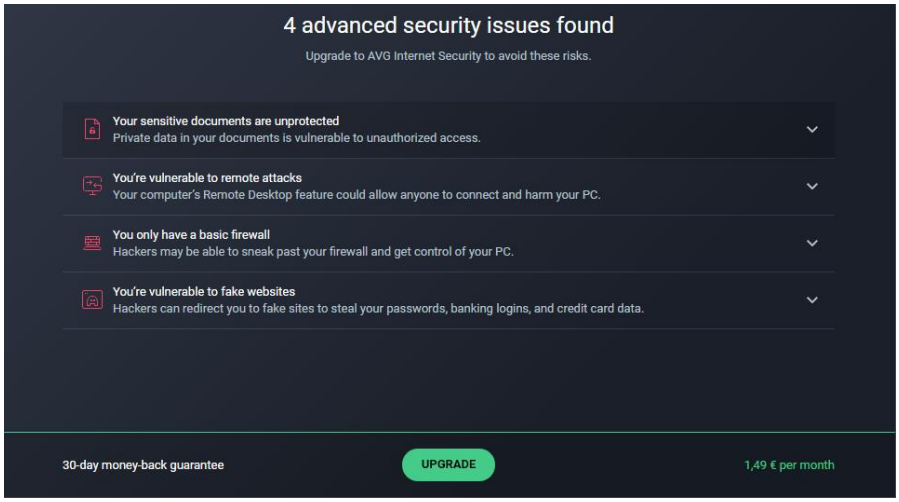

Figure 2. Example of fear appeal in software.

2.1.4 Protection Motivation Theory

Protection motivation theory (PMT) was first developed to explain fear appeals' effect on attitudes and behaviors related to health but has since its incursion been utilized in other areas such as political issues and environmental concerns (Floyd et al., 2000). The theory is also in use within the information security field to understand individuals' behavioral intentions when exposed to a fear appeal related to information assets (Boss et al., 2015). What is important to note is that a threat targeting an information asset does not necessarily pose any threat against the individual that is exposed to the fear appeal, but rather the organization of which they are a part. In information security, fear appeals are possible to implement to change end-users (e.g., employees, consumers, etc.) protection behavior related to their information assets, for example, private devices or information assets to which they have access, for example, a work computer.

The protection motivation theory is divided into two distinct cognitive mediating processes, the process for a maladaptive response and the process for an adaptive response (Rippetoe & Rogers, 1987). The maladaptive response can here be seen as an unwanted action and the adaptive response as an action that is wanted. The unwanted or wanted reaction is viewed from the perspective of the party that seeks to gain from implementing a fear appeal. The first cognitive process that is addressed is the one handling the maladaptive response as the threat needs to be recognized by the individual before the coping options can be addressed and evaluated (Floyd et al., 2000). Here intrinsic and extrinsic rewards of the maladaptive behavior are evaluated against the severity of the threat and how vulnerable the individual is to the threat (Rippetoe & Rogers, 1987). The rewards heighten the probability that the maladaptive response will be followed, while the threats lower the probability. An intrinsic reward should here be viewed as being personally rewarding, such as satisfaction from a good-tasting dish. Extrinsic rewarded on the other hand are externally rewarded, for example, peer approval, and not rewards that benefit the individuals surround-

ing. The adaptive response is evaluated after the maladaptive response. It follows the same logic as the maladaptive response with factors that increase the probability and a factor that lowers the probability; self-efficacy, response efficacy, and response cost. Self-efficacy is the individual's belief that they can successfully carry out the necessary action, while response efficacy is the belief that the action carried out by the individual is effective. Both increase the probability for the individual to adopt the adaptive response. Response cost decreases the probability for the individual to adapt the adaptive response and is what the individual perceives as the cost of the action, which could be time, money, and/or effort. The way to affect this cognitive process is to persuade the individual to choose an adaptive response by amplifying the fear that relates to the threat (Johnston & Warkentin, 2010).

2.2 Research background

Previous literature is here divided into three sections. The first section presents how PMT has been used to analyze users' behavior concerning personal devices. The following part looks into how PMT has been used to analyze fear appeal's effect on digital natives. The last section presents previous literature on how digital natives are using personal devices.

2.2.1 PMT and Personal Devices

How the fear appeals affect the individual concerning personal devices is described in previous literature as having two main components with various effects on the fear appeals, namely severity and vulnerability. The perceived severity of a threat is described as having a positive influence on individuals' intention to behave in a preferred way (Dang-Pham & Pittayachawan, 2015; Hovav & Putri, 2016; Thompson et al., 2017; Verkijika, 2018; Vrhovec & Mihelič, 2021). One important finding made by Thompson et al. (2017) is that perceived severity was only found to be influencing mobile device users. The claim that perceived vulnerability has a positive impact on user behavior is however disputed with findings to both support and dismiss the claim. Ameen et al. (2020) do not find any evidence that supports the claim that perceived vulnerability has any impact on behavioral intention when using smartphones. Another consequence of using the vulnerability in fear appeals is increased feelings of capitulation expressed by individuals, which can relate to continuous failures of security policies (McLeod & Dolezel, 2022). According to Vrhovec & Mihelič (2021), there is a difference between perceived vulnerability depending on the target (i.e. organizational or individual). Their finding suggests that the vulnerability directly targeting the individual can have positive effects on the individual’s behavior while the vulnerability of the organization does not affect the individual's behavior. Thompson et al. (2017) find similar evidence for perceived vulnerability when investigating users of home computers and mobile devices, where perceived vulnerability at home had a positive impact on security behavior.

Awareness of risks is a crucial part of security, but there is evidence in previous literature that this is an area that is lacking concerning mobile devices (Ameen et al., 2020; Ismail et al., 2017). A lack of perceived vulnerability can be tied to a lack of awareness of risks associated with the security of smartphones (Ameen et al., 2020). Ameen et al. (2020) further argue that this can indicate that there

is a lack of employee awareness programs. Ismail et al. (2017) present similar results tied to 12 advanced persistent threats occurring from repackaged applications and spearfishing. Self-efficacy has been shown to have a positive impact on security intention in certain studies (Belanger & Crossler, 2019; Thompson et al., 2017; Verkijika, 2018), while others show nuance in how this attribute affects security intention and behavior. Vrhovec & Mihelič (2021)find that the different coping appraisals work fully when the fear of cyberattacks is low but that especially self-efficacy has a positive impact on coping appraisals weakens when the risk is higher. This trend is not dependent on whether self-efficacy is high or low. A divide in the matter between gender and residency is reported by Ameen et al. (2020), where females in the USA reported that confidence in conducting security measures for their smartphones is an important factor. This behavior was not shown by the other respondents (males from USA, females, and males from the United Arab Emirates). Inconsistencies in self-efficacy are found by Dang-Pham & Pittayachawan (2015) as well but are here reported as being dependent on which context the individual faces risks. In this case, the respondents perceived self-efficacy as a stronger motivation to avoid malware in their university context than at home. In summarization perceived severity has been studied to impact users' behavior of personal devices. Perceived vulnerability and self-efficacy are two aspects that are disputed to which degree the impact user's behavior and in which contexts they are effective.

2.2.2 PMT and Digital Natives

Applied to the usage of personal devices the two factors that are meant to be impacted by a fear appeal are shown in previous literature to indeed affect the intention of users. There is a difference in how different generations behave, however, and this is elevated by Li et al. (2022) in their study investigating cybersecurity behavior. Their delimitations between generations are different from other sources by having one generation from 1980 to 1996 and one generation after 1996. What is displayed however is that there is a difference between perceived severity and perceived vulnerability when comparing the definition of digital natives and digital immigrants proposed by Perensky (2001). This is conflicting with the findings made by Roberts & Rahman (2021) that don't find a significant correlation between being a digital native and a different susceptibility to fear (i.e. threat severity and threat vulnerability) compared to other generations. An interesting difference between the two studies is that Roberts & Rahman (2021) target the vulnerability of the individual while Li et al. (2022) place a larger emphasis on the vulnerability of the organization that which the individual is involved.

Table 1

Contents of the protection motivation theory

Response	Factor	Probability	Cognitive Process
Maladaptive	Intrinsic Reward	Increasing	Threat Appraisal
	Extrinsic Reward	Increasing	
	Threat Severity	Decreasing	
	Threat Vulnerability	Decreasing	
Adaptive	Response Efficacy	Increasing	Coping Appraisal
	Self-Efficacy	Increasing	
	Response Cost	Decreasing	

Note. This table describes the components in the protection motivation theory described by Floyd et al. (2000).

2.2.3 Digital Natives and Personal Devices

Individuals with digital native status are more likely to be adopters of new technologies. IT consumerization is also affected by the rapid product cycles of consumer IT, which leads to larger dissatisfaction when employees are enforced to use old and incumbent systems (Ostermann & Wiewiorra, 2017). The dissatisfaction increases the longer an incumbent system is in place. Previous research is divided on the topic if digital natives' personal and professional lives are more intertwined or not (Jarrahi et al., 2017; Leuprecht et al., 2016; Shirish et al., 2016). Jarrahi et al. (2017) find evidence for a fading line between professional and private life by highlighting one company's social media policy that highlights that employees' actions in these environments have an impact on both their professional and private life. Leuprecht et al. (2016) argue that digital natives don't distinguish strongly between private and professional time and that they are less likely to recognize that different roles they take require different decisions. These views are in contrast to Shirish et al. (2016), who in their study found that digital natives view their professional lives as something that needs to be kept separate from their personal life. Weeger et al. (2020) do argue that the digital natives' specific individualistic and narcissistic traits, identified by Twenge & Campbell (2008), are further recognizable in their intention toward BYOD. This takes the form of trying to utilize all the possible benefits and neglecting risks that do not target them directly.

2.3 Fear Appeals to Influence Digital Natives' Device Usage

One of the main constructs that can be manipulated to form a fear appeal has in previous literature been articulated to positively influence users to comply with the recommended way to act is threat severity (Dang-Pham & Pittayachawan, 2015; Hovav & Putri, 2016; Thompson et al., 2017; Verkijika, 2018; Vrhovec & Mihelič, 2021). The other factor that can be influenced, threat vulnerability, differs in claimed impactfulness between different studies (Ameen et al., 2020; McLeod & Dolezel, 2022; Thompson et al., 2017; Vrhovec & Mihelič, 2021). These factors are not explicitly studied among digital natives in the role of an employee, however, but rather take a more general outset on fear appeals and

personal devices. Identified by Weeger et al. (2020) in their study of the intention to participate in a BYOD program digital natives do show that they are likely to be affected by risks that target them directly and are related to their mobile devices. They do not apply the PMT model to study the behavior, however. Furthermore, manipulation of threat severity and vulnerability for the usage of fear appeals is not used in their study. Li et al. (2022) claim that digital natives are the generation born after 1996. This is however a statement that is widely different from other sources including the referenced Perensky (2001), which all target some year in 1980 as the starting point for the generation that experienced the usage of digital technologies from a young age and later got called digital natives.

3 Method

The method chapter is split into five sections. The first section provides a brief description of two epistemological positions often applied in social sciences and provides reasoning as to why the chosen position was best for this study. Section two further provides details of which individuals were targeted for this study together with reasoning for why a qualitative approach was the best strategy for conducting this study. In section three a discussion of validity and reliability is provided with examples of choices made to increase these two aspects. Section four provides examples of ethical consideration that was done in this study. Lastly in section five an explanation of how the analysis of the data is outlined.

3.1 Research Philosophy

To properly describe the methodology utilized in this work, the positioning behind the study needs to be explained. As described in the background, digital natives have been described in previous literature to behave differently than previous generations and their behavior does not always correspond with how professionals in the field view them. IT, in general, has become more accessible for individuals which have led to trends where private devices can merge with the IT infrastructure among organizations. From an information security perspective, this can pose a risk. As highlighted by Crossler et al. (2013) different methodologies can broaden the understanding of how the fear of fear appeals impact individuals when utilized in the information security context. Furthermore, different qualitative approaches are underutilized when studying compliance with information security policies (ibid.).

The interpretative and positivist are two different epistemological positions on how to approach studies in social sciences (Bryman & Bell, 2013). According to the positivist approach, research in social sciences will only be able to reach the level of quality that natural sciences have in explainability, predictability, and control if natural science methods are applied (Lee, 1991). This is made possible by reducing the area of investigation to enable more accurate predictions and explanations (Braa & Vidgen, 1999). Social sciences in contradiction to natural sciences do however face problems in implementing a positivistic approach as social realities can be difficult to quantify, capture into formal propositions and test with experimental controls (Lee, 1991). Intercessors of the interpretative approach in social sciences argue that individuals and artifacts created by individuals are different from the artifacts studied in natural sciences and thus need to be studied in a different way (Lee, 1991). The main concern when applying the approach of interpretivism is to understand the view of an individual in a certain situation (Braa & Vidgen, 1999). The research questions formulated in this thesis are seeking to understand how digital natives view how they are impacted by fear appeals in their work environment. This correlates with the description of the interpretative approach as gaining an understanding of individuals in a certain scenario (Braa & Vidgen, 1999). Although the epistemological positions and the two research strategies qualitative and quantitative research are not the same or necessarily attached. Bryman & Bell (2013) argues that the two epistemological positions have close ties to one separate strategy of doing research, i.e. qualitative research has ties to the interpretative position and quantitative research have ties to the positivist position. These ties however

are not absolute according to Bryman & Bell (2013). They do however recognize that this is debated in the literature and that some authors indeed claim that the choice of research methodology does carry epistemological and ontological positions.

In this work, the perspective and social reality of the respondents are the keys to being able to further examine the behavioral intentions of said respondents. The reported emotions and influence they have on the respondent's decision-making are sought after, aiming to capture the nuance of the respondent's social reality. As stated by Crossler et al. (2013) this is an underrepresented approach to conducting information security research that can bring more nuance into the field. An adaption of the interpretive approach will thus be followed to fully capture the complexity that individuals' emotions and reasoning can entail. It shall also be noted that the qualitative strategy and the interpretive approach are not used interchangeably in this study although the qualitative method is applied and an interpretive approach to analyze the results is used.

3.2 Data Collection Method

This study utilized a qualitative method by conducting semi-structured interviews. The qualitative perspective is focused on humans' perception of their environment and to get insight rather than statistically analyzed facts (Bell & Waters 2016). This study is exploring the digital natives' perspective of how they are affected by fear and fear appeals, and the reasoning of the individuals to act in a certain way. The respondents' thoughts and reasoning are thus of importance. The interviews will follow a structure based on the PMT model incorporating all the aspects that are used to form protection motivation. This will then be formulated into questions relating to the usage of devices and the motivation for the usage of a certain device (private or corporate-owned). As advised by Boss et al. (2015) PMT will be used instead of some other model utilizing fear appeals as they argue that these models have the risk to end up weaker both theoretical and empirical. Semis-structured interviews were used as a data-gathering method since the analysis is conducted using a theoretical framework but is at the same time dependent on the ability of the respondents to elaborate on their thoughts on the matter. Thus, an interview protocol was formulated covering the parts that needed an answer from each respondent to answer the research question.

3.2.1 Selection of Respondents

The first decision made in regards to sampling in a qualitative study derives from the research question and conceptual framework (Farrugia, 2019). This further enables the researcher to draw boundaries of the study and further apply delimitations of the case. Qualitative methods are never random but are rather applied with the intent to understand a certain phenomenon (Gill, 2020). With this said several defined types of sampling can be applied (Farrugia, 2019; Gill, 2020). In this study, purposive sampling was applied as several delimitations were defined before contact was made with possible respondents. This type of sampling can be done when the author believes that respondents who fulfill certain criteria can provide critical information to answer the research question (Farrugia, 2019; Gill, 2020). The targeted respondent group was people born in 1980 and onwards as this is the group first described by Perensky (2001) to be digital natives.

This definition has been used in several studies since and will be used in this study as well. The argument for using generational has been debated, but Twenge & Campbell (2008) highlights the difference between generations by examining generational data from when each generation was of a certain age. This does diminish the possibility that maturity could have an impact on behavioral differences. In this study, only Swedish companies were contacted. The first and biggest possibility this enabled was that respondents were more likely to be able to conduct the interviews in their native tongue. As described in chapter 3.1 this study aims to understand the individual in a specific context and eliminating the possible language barrier between two non-native speakers or one native and one fluent speaker was considered one big part of understanding the respondent's answer. This further enabled the interviewer to follow up on different parts of the responses in a seamless fashion.

As the qualitative method is nonlinear (Morse et al., 2002), the method for selecting respondents was concurrently revised. The first stage of sampling of respondents targeted a narrowed-down group of people, described by Farrugia (2019) as a homogenous sampling that provides respondents with similar experiences and backgrounds. The criterion for selecting this first group of respondents was to target individuals working for a company adhering to the definition of Small and Medium-sized companies. The targeted companies were either providing and maintaining a digital product (i.e., software) or providing consultancy services within software development. The reasoning behind targeting these kinds of companies was the access to information from both the employer and customer, meaning that their actions regarding policies not only have an impact on their employer but also on different customers regarding information. The respondents were reached by sending out an email to 210 companies asking for respondents in the specified age group. This resulted in a response from four respondents.

After the first selection of respondents, one criterion got modified and one criterion got added. In interview four, the respondent provided information that even though he was employed by a company adhering to the SME definition, that company was included in a concern that implemented policies for several companies. The decision was made to drop the limitation of only searching for respondents employed by an SME company, as this would be irrelevant if the company was included in a concern implementing policies. The criteria that were added were to exclude people that had governance over what policies to implement. This was done because the scope of this study was to investigate what effect fear appeals could have on employees. To ask how individuals are affected by policies while they have governance over and have agency to change policies were considered redundant.

In the second stage of sampling, the first strategy was to reach out to companies by a phone call and a total of 45 companies were contacted, yielding zero results. This resulted in a pivot in strategy for contacting potential respondents. The shift was made from reaching out to companies to employing a strategy where individuals previously known to the author were contacted. This stage followed purposive sampling as the previous criteria were still followed when considering whom to contact, but in part also convenience sampling as it targeted individuals

that were easy for the author to get into contact with. A total of three respondents were gathered during the second sampling.

A third sampling was conducted in the same manner as the second sampling, with the exception that both convenience and snowball sampling were applied. The snowball sampling was conducted by contacting a respondent from the second sampling, asking if that respondent had any suggestions for other respondents. Even though snowball sampling was applied in this stage the last respondent was not reached through this method, but rather the convenience sampling. The third sampling resulted in one respondent, making the total of the respondent from all three sampling occurrences eight in total.

To summarize the characteristics of all respondents 3 tables with primary characteristics of the respondent group, not tied to individual respondents. This has been done in a pseudonymization effort to further enable the privacy of the respondents. As the author has knowledge about what specific individuals were interviewed, they cannot be considered to be fully anonymized but rather pseudonymized.

Table 2

Gender distribution of the respondents

Sex	Amount
Male	7
Female	1

As seen in table 2, both male and female respondents did partake in this study. What is important to note however is that there is a much larger representation of male participants than female.

Table 3

The decade of birth distribution of the respondents

Decade of birth	Amount
80's	3
90's	4
00's	1

Even though the decades 10's and 20's could be considered to be included in Prensky's definition of a digital native, these were not included as individuals born in these decades are not yet over the age of 18. This study targeted specifically people currently employed, these decades were not represented in this study. All reasonable decades to include in this study were represented, with a

larger representation in the 80's and 90's. The distribution is represented in table 3.

Table 4

Profession of respondents

Profession	Amount
Software development	6
Support	1
Business intelligence	1

As detailed previously a certain demographic was targeted for finding respondents. Although there were possibilities for different positions, there was still a limitation. In table 4, a representation of what work areas the different respondents were deriving from.

According to Saunders et al. (2017), saturation can be varied depending on what scope of the study. What is also argued is that saturation should be viewed as a spectrum, where a study can reach varying degrees of saturation rather than a point where saturation has been fulfilled, meaning that new data does not add to the overall theory. As this study investigated how fear appeals can affect digital natives through the lens of the aspects of PMT, saturation was seen to have reached an adequate level when no radically different answers were given to the questions. An example of what was considered a radically different answer to a question between sampling one and two was when respondent four expressed feeling strong emotions following an incident, which had not occurred with the previous respondents. Interview eight did not give any testimony that had a big impact on the overall theory but did add some nuance to the previous answers. Because of this, the study was considered to have reached an adequate level of saturation after interview eight and no further sampling was conducted.

3.2.2 Design of Interview Guide

To study the effect of fear appeals qualitatively, the choice was made to utilize semi-structured interviews. As described in section 2.1.4 the PMT model was first introduced to explain fear appeals' effect on health behavior but has since then been adopted into other areas (Floyd et al., 2000). Boss et al. (2015) have been critical of how the model has been implemented in information security research and propose that researchers shall use all of PMT's constructs before adding elements. The reasoning is that models omitting elements have not been tested with the same rigor as PMT. Because of this PMT was chosen as the basis for this study. Using PMT provides specific thematic points that needed to be investigated in each interview. As the focus of this study did take an outset on specifically mobile phones used, the questions were designed to incorporate the full PMT nomology concerning how the respondents used their mobile phones. The full interview guide can be found in appendix 1.

3.3 Reliability and Validity

The challenges to confirming rigor in qualitative studies are in contrast to the more straightforward capabilities currently available for quantitative studies (Morse et al., 2002). Lincoln & Guba provides two alternative criteria for verification of qualitative research, trustworthiness, and authenticity (as cited in Bryman & Bell, 2013). The trustworthiness houses aspects that can be seen as equivalents to the reliability and validity aspects of quantitative research. Morse et al. (2002), however, argue that there is a problem with establishing trustworthiness after the research is conducted and propose that the reliability and validation process of qualitative work should be intertwined with the research process at the same time as it is conducted.

Morse et al. (2002) propose five verification strategies to ensure reliability and validity during a qualitative study. First, congruence between the research question and the methods used to answer the question needs to be present. In this thesis, the questions were based on a previously established theoretical model which also in part were used for the analysis. Revisions of the interview protocol were conducted in discussion with the author's supervisor to further connect the protocol with the theoretical model (PMT). An appropriate sample is the second verification strategy presented by Morse et al. (2002). Seeking out people that can best represent views for the research topic is crucial to effectively saturate the categories. In this thesis, the sampling method had a specific focus on which respondents were desirable and is previously explained in subchapter 3.2.1. The third point presented by Morse et al. (2002) is to analyze and collect data iteratively, which forms an interaction between what is known about the subject and what needs to be answered. As described by Kiger & Varpio (2020) the phase in which transcription takes place the researcher can start to familiarize themselves with the data. In this study, the transcription took place between interviews and allowed for the author to formulate initial ideas about what information the data held and the major subjects the respondents expressed. This approach also enabled the author to conduct the fourth step presented by Morse et al. (2002), “thinking theoretically” (s.18), comparing the researcher's ideas with what respondents expressed. The last step presented by Morse et al. (2002) is to deliberately compare the data and the conceptual understanding.

3.4 Ethical Considerations

When reaching out to potential respondents for the interview, the company at which they were currently employed was contacted, fulfilling the criteria for the respondent's age and company size. If the company confirmed that the company had a potential respondent, that respondent was further contacted. A brief introduction of the author, the purpose of the interview, and permission to record the interview were sent to the respondents. When reaching out to potential respondents previously known to the author the same information regarding the study was sent out. No contact through the employer was done when reaching out to individuals previously known by the author.

When the interview was conducted the respondents were asked once again for confirmation that it was okay to record them. The respondents were also asked if they wished to withhold personally identifiable information such as name and name of employer etc., with the logic that if one respondent wished to withhold

this information about themselves all respondents would be treated in the same way. The respondents were informed that the recording was only meant for transcription purposes and was audio-only. All interviews were conducted via videocall. An active choice was made to not utilize any transcription service to not accidentally leak any personal information about the respondents. Moreover, all interviews were saved and processed locally i.e., cloud storage was not utilized.

The choice to study only one delimited age group is based on previous research studying generations and partially practicality. As proposed in several previous studies (Bennett et al., 2008; Helsper & Eynon, 2010; Jones et al., 2010; Twenge & Campbell, 2008) digital natives have previously been recognized to behave differently compared to previous generations. The choice to only study one generation is based on the ability to conduct longer interviews within the allotted time for this study. This is to get a more nuanced data set that can include a richer description of the respondent's perception of how emotions impact their decision-making. Digital natives were chosen for this study as they are the generation that has the most time left of their work life. Because of this, it is important to view this study as patterns found among digital natives (see definition in section 2.1), which necessarily don't repeat in age groups outside of this definition.

Another aspect to consider when viewing the results from this study is that the respondents were working in the IT field (exact sampling of respondents in section 3.2.1), which could influence the answers. Why this group was chosen however because their jobs include accessing customers' data in different ways. Because of this, their actions do not only influence their employers but also their customers in a direct way. The case could be that their work roles have affected how they perceive and become influenced by stimuli such as fear. At the same time by delimiting which respondents to contact, a result with a more accurate representation could be reached.

3.5 Data Analysis

The PMT along with variations (e.g. the fear appeals model and technology threat avoidance theory) have been utilized to study fear appeals' impact on individuals related to information security (Boss et al., 2015). What often has been omitted is to utilize the full nomology of the PMT model before adding non-PMT constructs. Boss et al. (2015) do argue that this approach tends to end up weaker both theoretically and empirically. Because of this, a deductive analysis was chosen to understand how the respondents' perspectives adhered to the different parts of the cognitive process included in PMT. The analysis followed the guideline steps lined out by Braun & Clarke (2006) namely; familiarizing yourself with the data, generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the report (p.87). The first phase, familiarizing yourself with the data, is conducted to get a general idea of what the data includes. Here the first notes regarding patterns should be made and initial ideas for codes are forming. Phase two, generating initial codes, is the action of searching for labels to put on the different extracts of information retained in the interviews. Several codes do eventually end up and form a more overarching theme. In phase three, searching for different themes, codes are combined to form different themes and sub themes. At this

stage the different themes and codes start to form a thematic map. In the deductive part of this analysis the PMT will provide the overarching themes that the codes will adhere to. Phase four, reviewing the themes, the themes are analyzed and reviewed to determine if each theme holds enough data to form a theme. In this step the themes can break apart or merge into a new themes if they do not hold enough information. The themes should be coherent internally and with a distinct separation externally against other themes. In this study the codes were further revised and correlation between the PMT model's constructs were further examined in order to determine if the code adhered or not. In phase five, defining and naming themes, the themes are given their concreate definition and name. In this study the themes that did not adhere to any part of the cognitive processes defined in the PMT model were given a name and definition. Phase 6, producing the report, is described as the act of telling the story the data provides and further provide arguments in relation to the research question. Braun & Clarke (2006) do however state that this is not rules, but more of a guide and needs to be applied in a flexible way to fit the data. The guide should also not be followed in a linear way but should rather be recursive back and forth between the phases.

3.5.1 Deductive Content Analysis

A deductive thematic analysis adopts themes based on previous theory (Kiger & Varpio, 2020). PMT was used in this study both to formulate the interview protocol and to deductively analyze the results. Crossler et al. (2013) have proposed that to gain a greater understanding of individuals' behavior towards compliance with information security, studies should apply methods other than surveys or experiments. Because of the ability to gain a larger insight into individuals' reasoning by conducting a qualitative study in the form of interviews, the results were directly interpreted against the different cognitive aspects of PMT (see table 1). The ability for respondents to further explain their behavior enabled a deeper analysis of the behavior intent of the individual, contrary to a survey. It shall be noted here that PMT is only used to conclude if the behavior intentions expressed among the respondents concerning fear appeals can be tied to any of the steps in the cognitive processes. There is a possibility that the respondents do not experience any direct emotion to their intention to behave in a certain way, as proposed by Warkentin et al. (2016).

3.5.2 Inductive Content Analysis

In inductive analysis, the themes are derived from the data itself and can at times stride away from the question asked (Kiger & Varpio, 2020). Another important point is that the inductive themes don't have to align with the researcher's own beliefs on the topic (Braun & Clarke, 2006). An inductive analysis method often focuses on generating theory rather than proving the theory (Bryman & Bell, 2013). The inductive part of the analysis is in this study utilized to identify sub-themes within the aspects of PMT.

4 Results

PMT provides seven factors that impact whether an individual will choose the coping appraisal or the threat appraisal in response to a threat. These factors are presented in table 1 and will be used as the main themes in the presentation of the results. Within each theme, an inductive approach has been used to find the sub-themes that correlate with the overarching theme.

To further obfuscate the respondents only a description of the overall data set will be provided. The respondents were born somewhere between 1980 and 2002. The respondent used either a phone with the Android or iOS operating systems or both. The respondents used either a private phone, work phone, or work phone with two sim cards or both a private phone and work phone. Individuals defining themselves as male or female were participating.

4.1 Intrinsic Reward

For the intrinsic rewards, two themes were identified. First, the results tied to convenience will be represented under 4.1.1. The results tied to control over the divide between personal and professional usage will be presented under 4.1.2. Lastly, a summarization of both subthemes tied to intrinsic rewards will be presented in 4.1.3.

4.1.1 Convenience

Most of the respondents, seven out of eight, are using one phone. Respondent 3, 5, and 6 that only uses a phone provided by their employee explicitly state that they only use one phone for the convenience of not needing to switch back and forth between two phones.

"At my last place, they asked if I wanted an extra [phone] only for work. I tested it and thought that it could be pleasant to not get a lot of mail to my private [phone]. But it got actually more difficult I thought and cumbersome. Because then you have to keep track of two phones. […] So when I switched jobs they asked me and then I said that I prefer to take everything on the same [phone][…]" – Respondent 3

Respondent 8 has chosen to use one phone because then he does not need to purchase a private phone. He only sees drawbacks with using one phone for both private and professional tasks, except for the gain of not needing to buy a private phone.

"I think that it only carries drawbacks to have one phone. But not enough for me […] to buy my own phone" – Respondent 8

The two respondents who currently only have access to a private phone have not been supplied with a phone from their employee. They still have the option to access some work-related information or communication through their private phone and have utilized this option for convenience.

"[…] I have just now installed Teams. It is completely optional. It is nothing that is required. It is only that I have noticed that it is very convenient to have

Teams on the mobile phone. […] it can be at lunch or exercising […] it can be nice to write to people. Who actually is at the office." – Respondent 7

Respondent 7 has encountered previous work situations where a work phone was obligatory. This resulted in a situation where he only used his work phone for both private and professional use because of the convenience.

"[…] I always had a private [phone] where I did not install anything work-related. However, it became that my work phone kind of. I kind of switched numbers and used it as my primary phone. So everyone could reach me at that one. I always had it on me because I did not bear to have two." – Respondent 7

Respondent 1, who has access to one private and one personal phone, uses both phones in work-related matters out of convenience as well.

"[…] because I have an Android [private] and an iPhone [professional] it is convenient to use them both for testing." – Respondent 1

Even though the respondents have different configurations of mobile phones, the major aspect tied to intrinsic reward in their usage of their mobile phones is how convenient it is to use. Respondents 3, 5, 6, and 7 also state that the primary aspect impacting their behavior with their mobile phone is how convenient it is to use.

"[…] if it is something, I don't know, that makes my everyday life more effective. And make it more smooth, then I will probably use it." – Respondent 5

4.1.2 Individual control

To have a divide between private and professional life is an aspect valued by respondents 1, 2, 5, 6, and 7.

"[…] there is a much higher risk I feel. That you get worn-out in another way[…] Now I was free from work a little while back and there was this colleague that reached out and needed access to a place. It was good that she could reach me. But at the same time, I was free from work." – Respondent 6

Respondents 3 and 4 perceive that they have full control over the work interactions outside of working hours, resulting in them not being bothered by work interactions taking place when they are free from work.

"It does not have any effect in that way [being disturbed by having a work-mail on a private device]. And I can choose to remove my mail from my private phone" – Respondent 4

The respondents using one phone tend to use it sparsely for work-related matters and more for private tasks, even in the cases that the phone is provided by the employer.

"I see the phone as my personal phone where I also can do some job stuff" – Respondent 5

4.1.3 Summarization of intrinsic rewards

To summarize the results for intrinsic rewards there were two sub-themes found. Convenience was brought up as one of the main aspects that the respondents cherish in their usage of a phone. To be able to have access to effective solutions and tools that help the individual in a way that they perceive as effective is a part of what the individual perceives as having an impact on their behavior. The second aspect is the individual's control over their time off and their time at work. Even though this aspect was split between not getting disturbed on their time off and being involved in work at their free time at their own pace, this aspect still fits into being able to control their free time.
These two aspects can be rewards that can pose as a reward for maladaptive behavior, for example when abandoning a private phone when it is seen as inconvenient to carry around two phones.

4.2 Extrinsic Reward

The aspect of convenience in the usage of mobile phones is prevalent regarding how well the respondents perceive that they can carry out their work as well.

"I think it helps a whole lot to get notices and reminders. […] I can answer directly." – Respondent 4

As there to date are two operating systems that are the two main competitors, android and iOS, the possibility for a developer to test their artifacts on both environments. This can enhance the employee's performance in their work environment.

"[…] because I have both an Android and an iPhone it is convenient to use both in testing" –Respondent 1

Solutions that are required to be used by the respondents to conduct their work, e.g. two-factor authenticator, are being used on the respondents' phones. This is done no matter if it means that the phone is privately owned or is being provided by the employer.

" It does not matter if I am at work or not. I do open it [the phone] and use it in the same way. It is only that I have chosen to put certain apps further back in the pages" – Respondent 3

Solutions that help the respondents adhere to security directives, e.g. password managers, are also utilized. The respondents are however using these solutions in a phone environment that mixes private and professional usage.

"[…] if my password would leak, I would still not compromise my accounts at [customer] in this case." – Respondent 2

The behavior that can be connected to extrinsic rewards is when the respondents are utilizing solutions that enable them to heighten their work performance. These solutions are utilized no matter what mobile phone environment they are implemented in, i.e., private or professional. The first scenario where the respondent use tools connected to work in a mixed environment is when the tool is a requirement from the employer or work task that the respondent

needs to carry out in their professional role, e.g. two-factor authenticator. The second scenario when this can occur is when the respondent utilizes a tool to act more securely, e.g. password manager.

4.3 Threat Severity

Two subthemes were found for threat severity. Under section 4.3.1 the first subtheme is presented and the results tied to what the respondents do perceive as a severe consequence that can occur from a threat. Findings related to anecdotal evidence as a factor that affects behavioral change are presented in section 4.3.2. A summarization of threat severity is given in section 4.3.3.

4.3.1 Perception of severity

What the respondents perceive as severe consequences that can occur from an incident is nonunanimous. Respondent 2 perceives the most damaging threats as the ones that target his funds.

"[...] but often it is nothing more sensitive. It has not been with money involved. Thus far. But it can be. [...] It can have very large consequences." – Respondent 2

Another concern is raised by respondent 1, pointing towards privacy to be the biggest issue and who is the owner of what can be viewed as private or personal information. In this case, the most severe threats are targeting the individual and can be threats that arise from an employer.

"The clear downside is that it is not my phone. So, everything that happens on it is owned by my company or the company that I am working for. [...] So, I am very aware that my private conversations should absolutely not be available to my company." – Respondent 1

4.3.2 Impact of anecdotal evidence

Anecdotal stories of threats and incidents that can occur in the phone environment do seem to have an impact, while still not triggering any specific emotion. This is even though the severity of the threat is perceived as carrying large consequences for the respondent.

"[...] I heard a story of someone that got scammed for money because they key in their bank id at the wrong time. After that, it became a mechanical thing. My eyes travel up one last time. Before I press ok." – Respondent 8

Incidents that do not result in any visible loss for the respondent do not trigger any emotional response. Even if the respondent does change their behavior following an incident of this visibility and scope, the respondent does not experience any specific emotion. Respondent 3 describes that there is no direct emotion connected to having his passwords leaked, but rather to having the task of changing the passwords.

"[...] now I know that I must do this. Because it was not strong enough and I maybe had used the same password at multiple places. I would not say that

there is a strong emotion associated with it more than that I have more work to do." – Respondent 3

One respondent describe an incident where he got scammed for money and the emotions associated. The respondent describes their feelings connected to this occasion as despair and shame rather than fear.

"Then I felt proper despair. What was I thinking? How stupid am I? Those feelings." – Respondent 4

4.3.3 Summarization of threat severity

To summarise there are two main points extracted from the data. The first is that what is perceived as a severe consequence is different from respondent to respondent, where some respondents point out that their largest concern is the threats that target their monetary funds while others point toward the disclosure of their private information. In the case where private information disclosure is perceived as the more severe threat, the respondents can be more concerned with what information the employer owns.

The other point is that anecdotal evidence of threats or incidents that have occurred but only resulted in non-visible or abstract severity do trigger a behavior change. In these cases, the respondents do not report that they have any emotion connected to the occasion. One respondent has encountered what he reports as feelings connected to an incident, but none of the emotions were fear.

4.4 Threat Vulnerability

Three subthemes were recognized for threat vulnerability. The first sub-theme was connected to the respondents' view of mobile phones and is presented in section 4.4.1. In section 4.4.2. the respondents' views of how policies affect their mobile phone usage are presented. What effect fear have on the behavior of the respondents is presented in section 4.4.3. Lastly, a summarization of threat vulnerability is given in section 4.4.4.

4.4.1 Characteristics of mobile phones

The general perception of mobile phones is that they inherit similar characteristics that can be found in a classical computer i.e., desktop or laptop computer. Even if the respondents do not necessarily know what concrete threats that can explicitly target mobile phones. The general perception is that the mobile phone is a computer and because of this logic they should inherit similar vulnerabilities and flaws.

"One of the biggest problems today is malware that enters your phone or your computer for that matter. […] It is easy to forget that the phones of today are more powerful than the computer you had 10 years ago. […] You can connect some thousand phones and get a pretty powerful botnet." – Respondent 1

Even though the inheritance from traditional computers is clear for the respondents, they do still perceive that mobile phones have some characteristics that separate the ordinary computer environment from the mobile phone environment.

"[…] the phone feels more like a communication device than a computer. Mabey more of a specialization[…] you have SMS and calls. That you don't have on a computer in the same way." – Respondent 7

This is further reflected in the answers regarding what threats can target mobile phones in general, where the respondents have a good perception of what digital threats are available. They also explicitly state that these threats apply to the mobile phone as well.

"I do not have any concrete targeting mobile phones. […] More than the general threats like man in the middle attacks for example. […] Else malicious software that can enter your phone when you download an app[…]" – Respondent 3

4.4.2 Policies for mobile phones

The respondents are exposed to policies that are formulated in a general way, forcing the respondent to interpret what does apply to their mobile phone usage and what does not. An example of this is the difference in respondents 6 and 7 regarding policies that have shaped their mobile phone usage.

"[…] when I am traveling and are supposed to work at a train it has become, because we have a lot of rules regarding that you are not allowed to connect your computer to a public network. It has become so that I am connecting to my phone." – Respondent 6

This view of what policies applies to mobile phone usage is in stark contrast to respondent 7 that are more concerned with breaking rules regarding copyright infringement.

"[…]I maybe should not take a link from YouTube and send it on Teams. I rather write the song with this band. […] And think about licenses for different things." – Respondent 7

This is further expanded when the respondent reminisces what he has encountered in previous employment. Here the respondent recalled that his employer was heavily concerned with copyright infringement conducted on the company's computer as this would impact the company and not the individual conducting the infringement.

"[…]from my first job. When I had a computer which I used more for private matters and a mobile which I used more privately. That my boss said that we were absolutely not allowed to have any pirate copies or anything we did not have licenses for. Because then the whole company would get caught." – Respondent 7

4.4.3 The effects of fear

The respondents do not demonstrate any feelings connected to fear when they give examples of encounters where they have experienced or been informed of the vulnerability of threats that can target their mobile phones. Respondent 2 reminisces a demonstration of hijacking a mobile phone where the perpetrator

got access to the whole phone. This is described as heightening his awareness of how easy it can be to be exposed to this kind of threat but does at the same time describe his experience as not necessarily invoking a sense of fear.

"It was an eye-opener. That one got nervous is the wrong word. One felt a little bit like, wait a minute. Has this happened to me? No, it has not. Can it happen to me? […] And then the same thing applies that I talked a little bit about before that one should have awareness about what mail one gets and what the mail asks of you […]" – Respondent 2

Respondent 1 has encountered colleagues, which he describes as highly experienced, of what possibilities and exploits exist regarding threats against the IT environment in general. He is still reluctant to describe his feelings as fear-related.

"I think some stuff I learned I got astonished by that it was possible to do. No not fear. It is a heightened awareness of risks. I don't know if it is fear that emerges. Maybe respect? No, not fear. Because then you act differently." – Respondent 1

This is reflected by respondent 4 who points out that his awareness and behavior are more easily influenced when encountering people with a claimed expertise. Even though information regarding threats that can occur unless precautions are taken does influence the behavior, the respondent does not experience any feelings associated with fear.

"It was a real eye-opener. […] If I would have heard it from a friend it would have been like. That is good so to speak. But when you hear it from a person like that, it becomes something different. It becomes like, oh shit! I think it is best that I do that." – Respondent 4

An incident revolving around leaked passwords did not invoke any sense of fear in the respondent. The response is described as logical rather than including any feeling and invoked a sense of a task to be done rather than an incident to be frightened of.

"[…] now I know that I need to do this. Because it was not strong enough […] I would not say that there is a strong feeling associated more than there is more work in front of me." – Respondent 3

4.4.4 Summarization of threat vulnerability

For threat vulnerability, three sub-themes were recognized. The first subtheme that was recognized where that the respondents viewed their phones as computers, inheriting the same vulnerabilities to threats as desktop or laptop computers. This indicates that the respondents are aware that the threat landscape is similar to the possibility for executables to carry infection but also that the threat of potential incidents deriving from connecting to public networks or clicking links in suspicious emails is as possible on a phone as a "classical" computer i.e., desktop or laptop.

The second subtheme found was that the respondents do not perceive those policies they encounter are stated to apply to mobile phone usage. Thus, the respondents perceive that they do need to interpret what policies do apply to their mobile phone usage, resulting in a diverse perception of which policies to apply. Even though the respondents recognize that a computer and a mobile phone have similar characteristics, which policies to apply to the digital environment are dependent on the respondents' previous experiences. This applies to the mobile phone environment as well. There are also accounts among the respondents that there are no policies in effect at all. Lastly, the respondents do not communicate that they experience fear when encountering stimuli that propose threat vulnerability of their mobile phones.

4.5 Response Efficacy

There is an element of trust in how the respondents choose which services to utilize. Even though there is a recognition that trusted service providers can include potential harmful elements.

"Install apps from the play store. You must trust google. But then it could be that junk can enter that way as well […] I try to use as official sites as possible. And not much else […] try to stick to the known sphere." – Respondent 2

To place trust in service providers is not synonymous with the belief that the service provider can protect the user from any form of harm, however. The user still needs to be aware that the platforms they utilize can include security flaws.

"I can not do so much about security flaws in Android itself, but I can at least refrain from installing apps I do not absolutely need" – Respondent 1

The previous statements are pointing toward the usage of Android phones. Respondent 3, who is using an iPhone, does have a lot more trust in the operating system and the apps available in the Appstore. This does, however, only apply to the specific threats of each operating system, not the general digital environment.

"You almost feel embraced by, what to say, the system." – Respondent 3

The respondents perceive that they need to place trust in service providers to use services. If this is trust in the efficacy of the responses or not is however not stated.

4.6 Self-Efficacy

It is described by the respondents that there are certain actions one does not take in a digital environment. An example of this is to click on links that the respondents perceive as suspicious.

"It is a lot that inherits from the computer environment. And there I am aware that one does not press all the links one gets. […] Just ignore it if you don't know whom it is." – Respondent 7

The ability to navigate and get accustomed to digital environments and their dangers have been introduced at an early age for the respondents. These have acted as lessons for the respondents on how to behave in a digital environment to not be exposed to any perceived threats.

"If I get an email that looks weird. Then I check if the email address looks okay. […] I will blame all the uncountable hours I spent on the internet. […] I got viruses when I was young and clicked on everything." – Respondent 8

When the respondents explain how they would handle an incident their self-reported approach for coping is first and foremost to cut off the possibility of communication for the targeted device.

"One can also turn off Wi-Fi and cellular data so that no information leaves the phone. So that is probably what I would have done." – Respondent 2

Depending on the respondent's perceived technical proficiency the second course of action is to either gather more information to get a clearer picture of what is the characteristics of the incident or to contact a trusted party that can help the respondent to fix the phone.

"I am fully aware that I am not an IT technician. So I think that I would contact my brother that is much better at it and ask him what to do." – Respondent 6

For the respondents with more self-perceived technical capabilities search engines on the internet and forums would be important tools to understand and fix a potential problem.

"I would definitely try to gather more information. Is it a bug in my version of the software or is it a serious flaw in the hardware? That one could exploit. […] I would probably hang out on stack overflow and check what people had to say" – Respondent 3

A response that is not described as communicated by the employer but still utilized by the respondents is to separate sensitive work information and private information by using the company-provided computer for work and mobile phone for private matters. This is conducted even if the phone is provided by the employer.

"If I would lose the phone or anything like that. Then I know at least that that information is not lost or have gotten into the hands of someone […]" – Respondent 5

The respondents perceive that their awareness of threats is an effective tool to combat incidents. This awareness has improved over time as they have encountered incidents from an early stage in life. They do also perceive that they are aware of their capabilities and limitations concerning how to handle incidents that could occur.

4.7 Response Cost

As described under the category of intrinsic rewards, the respondents want their usage of their mobile phones to be convenient. Because of this a lot of the perceived response cost is connected to when policies are tied to precautions that make the phone more inconvenient for the respondent to use.

"Rather that it has been much more cumbersome because we have so many security programs. It is always at least two steps." – Respondent 6

Even though the respondents think that certain precautions are bad ideas they are willing to utilize them if they think that the alternative is inconvenient. An example of this is respondent 8 who is reluctant to use biometric data but still utilizes this because of the convenience compared to being forced to use an eight-digit numeric code.

"You need to have a numeric code now. And it is a lot more cumbersome than what I had before. […] So, I put in fingerprint and face recognition in order to not be forced to press my phone eight times every time I want to open my phone." – Respondent 8

Responses that the respondents perceived as logical to implement and to have a direct positive effect on their work environment are not met with irritation but rather unconcerned or even positive attitudes.

"[…] when it comes to stuff like that when it concerns security and such it is almost finally from my point of view. Not that it is cumbersome but rather that this is something we should use, of course." – Respondent 2

The perceived response cost is dependent on if the respondents perceive the response as necessary or if the response is cumbersome for the respondent. Responses that are perceived as logical are not met with irritation or frustration by the respondent. If the respondent is met with a response that is perceived as cumbersome, the respondent will still comply with the solution but will try to find ways to meet the bare minimum of the requirement. In both cases, the respondent will, however, comply with what is required of them.

5 Discussion

This discussion is divided into six parts. First, in 5.1 some preliminary conditions described by the respondents about their current work environment, that have an impact on the respondent's susceptibility to fear appeals. In 5.2 a discussion regarding what effect fear appeals could have if implemented intending to change digital natives' behavioral intentions regarding mobile phone usage. The behavioral intentions of digital natives will be discussed in 5.3. The ethical and societal aspects will be discussed in 5.4 and 5.5 respectively, followed by a discussion of the study limitations in 5.6.

5.1 Ability to implement fear appeals

When looking into whether fear appeals are possible to implement not only the mindset of the one affected by the fear appeal is important but also how it would be implemented. When it comes to security policies regarding mobile phone usage no respondent stated that they had an experience with policies targeting mobile phones directly. Because of the perception that mobile phones are computers the respondents, however, view that policies regarding information and cyber security apply to their phones as well. This implies that the digital natives need to interpret what policies apply to the mobile phone and which ones do not. This is seen with respondent seven's answer that he applies copyright policies to the phone environment, which is not reflected among the other respondents. There seems to be a lack of clarity regarding what policies apply and how they should be applied to mobile phones. As stated by Ameen et al. (2020) awareness is a crucial part of security, but without having a conformed view of what does apply to mobile phone security the digital native is likely to reside to what their previous experiences have entailed.

Only two out of the eight respondents did perceive that they had regular training in information security and/or cybersecurity. As stated by Boss et al. (2015) fear appeals need to be used for longer periods to affect the recipient of the fear appeal. This means that lack of continuous training is another aspect that would be needed to change to effectively apply the fear appeals. In this case, the fear appeal would be a longer investment into the employee to strengthen the company. The company wanting to implement fear appeals would thus be forced to invest time and resources in an endeavor that would take a longer time to provide any benefits.

5.2 The effectiveness of fear appeals when applied to digital natives

How convenient the phone is to use is the basis for why many of the respondents choose to use only one phone. Two reasons for the respondents who chose to only have a company phone were either that they did not want to buy a separate private phone because of the cost or that they did not want to carry two phones because of the inconvenience of keeping track of two phones. The solution to not wanting to carry two phones could be to implement MDM or EMM (Siddique et al. 2020). Only one of the respondents had encountered this and his statement shows that this had been implemented poorly, resulting in a situation where he still had work information in his private mobile environment.

Because of this, unnecessary problems can arise because the configuration of devices and management of devices is carried out poorly.

Important to note is that the respondents perceive that the convenience of carrying only one phone is applied to both intrinsic and extrinsic rewards. The personal gain of only needing one phone is that carrying two phones does not become cumbersome and demands more effort from the respondent. The perceived extrinsic reward that can be gained is tied to how well the respondent perceive their performance capabilities in their work. Certain work tasks become easier to conduct, for example, respondent one who uses both his personal and private phone for software testing.

What threat is perceived as severe is different between different individuals. In this study either monetary harm or harm to one's privacy were perceived as the most severe threats by the respondents. In the case of harm to the privacy of an individual, the respondents perceive that they can not only be harmed by outside parties but also their employers. Looking back at the previous discussion under 5.1 about the potential problems with policies, it is clear that a fear appeal targeting digital natives would need to target different kinds of threats as the digital natives do not have a collective view of what threats are the most severe.

When looking into how the respondents perceive threat severity, no one experience the emotion of fear connected to the severity of a threat. This correlates with Warkentin et al. (2016) findings that fear does not motivate end-users to act more securely. The respondents still change their behavior intention when influenced by incidents or accounts of incidents. This enables the possibility that fear itself may not be the most effective way to influence digital natives to change their behavior regarding the usage of mobile phones.

When it comes to threat vulnerability the digital native does not report that they experience any fear either. This entails that fear is not an emotion that is experienced in connection with either the vulnerability or severity of a threat. The sheer amount of experience the digital native has accumulated by utilizing digital tools from an early age is reflected in their view of threats against modern phones. They view the modern phone to be more of a computer than a *"[…] dumb phone from the 90's"* (Respondent 1) and are also well aware that a modern phone has the same vulnerabilities. Many of the threats that can target a phone today are thus threats that the digital native has been accustomed to and been forced to adjust to from an early age. The digital native does rely on and trusts in their ability to detect potential threats and perceive themselves to have a good understanding of what threats are possible and not.

For a fear appeal to be effective the vulnerability and severity need to be manipulated in such a way that the individual affected by the fear appeal takes the recommended action (Boss et al., 2015; Johnston & Warkentin, 2010). As the digital native already perceive that they have a good understanding of threats that can target the digital environment and perceive that they do not experience any fear in relation to threats or incidents, fear appeals seem like an ineffective way to change their behavior.

When the respondents talk about how effective they view different security solutions or systems they express that a certain amount of trust needs to be put in the tool, system, or service. The trust the respondents are experiencing is not always expressed as a genuine trust in the solution but rather that they are not given any other choice but to trust the solution. Here they do express that even if you use a solution, you still need to be aware and open to the possibility that these solutions can change or get compromised. As described previously the digital natives have a lot of previous experience from using computers which they then have applied to the mobile phone environment. Whether or not a digital native will perceive a solution as efficient is dependent on their previous experiences. What is important to note is that there is a consensus among the respondents on certain things one just doesn't do in a digital environment, e.g. click at links in suspicious emails. This indicates that uniformity can be found surrounding the efficacy of certain responses.

The respondents are aware that they have limitations in dealing with certain aspects of self-efficacy of responses. Their perception is that even if they are not capable to fix a problem themselves, they can seek out the right help. This could be connected to their experience in seeking knowledge and having a basic understanding of the digital environment enables them to be efficient in applying or seeking solutions.

5.3 Digital natives' behavioral intentions

The respondents' behavioral intentions do not correlate with the findings proposed by Weeger et el. (2020) that the digital native would not care about threats that are targeting their digital surroundings. What seems to be the issue is that the digital native perceives to have a good understanding and experience of what threats are available in the digital environment and tries to utilize their perceived knowledge to the best of their capabilities. This is exemplified by respondent eight's reflection *"[...] I will blame all the uncountable hours I spent on the internet."* in relation to experience gained throughout the years of threats in the digital environment. If this perceived knowledge correlates with the recommended actions depends on how the policies are implemented and what training the employer provides. This is seen in statements such as *"Not that it is cumbersome but rather that it is something we should do, of course."* provided by respondent two in relation to when security measures are implemented that he has previously encountered, or "*Then I know at least that that information is not lost or have gotten into the hands of someone [...]"* provided by respondent five concerning choosing not to have what is perceived as sensitive company information on his phone. One finding in this study is that digital natives have a unified view of certain important aspects. The first aspect is how the digital natives view and use their mobile phones. The mobile phone is a highly important device that is integrated into everyday life, both professionally and privately. Even if a digital native doesn't get access to a phone for professional use, they are inclined to use their private phones to properly or more efficiently conduct their work tasks.

The second aspect is tied to how private and professional entanglement is viewed. Leuprecht et al. (2016) found that digital natives do not distinguish strongly between their private and personal life while Shirish et al. (2016) found that digital natives view their professional life as something that needed

to be kept separate from their personal life. What is found in this study is that digital natives don't want their work life to get mixed up with their personal life. What is also stated is that they do not feel that this is an easy task. This means that what the digital native wants and what occurs do not correlate. As described by Brodin (2016), private device usage may harm the employer.

The third aspect is that certain unified perceptions about security measures are ingrained in the digital native's behavior intentions. What is hard to find out is if the digital natives have accumulated this view because they are born into a digitally enabled world. As pointed out by Helsper and Eynon (2010), the case could also be that the accumulation of experience could affect digital native status. Then the question becomes if experiencing cybersecurity and information security have different impacts on an individual in different stages of that individual's life. No matter the case, what can be determined from this study is that digital natives have certain perceptions of security behavior intention related to the mobile phone environment and that these views are inherited from the computer environment.

5.4 Ethical Aspects

The main ethical consideration that impacted this study was to create conditions enabling usable data for analysis while at the same being acceptable for the respondents partaking in the study. Ellersgaard et al. (2021) claim that anonymity can enable higher validity in the data when a sensitive matter is handled. As this study partially concerns how the respondents behave concerning information security in their professional roles, testimony about behavior that does not align with the employer's preferred behavior could potentially carry repercussions for the respondent. Because of this, the respondents were asked if they wished to withhold information such as their name and the name of their employer etc., with the logic that if one participant wished to be treated in this way it would apply to all respondents.

To counter the issues with pseudonymization of the respondents a detailed description was provided as to how the sampling was conducted and what demographic was targeted, see 3.2.1. Following the provided details about demographic, similar individuals should be able to reach.

Looking into the ethics of the results reached, one could argue that manipulation or intention to manipulate individuals depends on what the intention of the manipulation is. The results reached in this study, indicate that fear appeals don't have any effect when trying to affect digital natives' security behavior with their phones. What is instead suggested is what aspects the digital native perceives as important for their behavior. In this context, the intention is to affect the digital native's behavior in such a way that it becomes more secure. Thus, studying the behavior in this context can help both the individual and their employers to benefit from a more secure digital environment by getting a bit more understanding of how to enable more efficient ways to enforce security.

5.5 Societal Aspects

First, this study indicates that usage of fear appeals is ineffective when trying to impact the security behavior with mobile phones among digital natives. Thus

organizations should avoid focusing resources on implementing fear appeals to change digital natives' behavior in this regard. As Boss et al. (2015) state, fear appeals need to be included during longer periods to have an effect. What seems to be a better approach is to make the convenient way more secure and accessible. An example of this is to put more resources into securing mobile phone environments by implementing MDM or EMM (Siddique et al. 2020). As found in the results, digital natives may disregard having two phones. A single phone still needs to be divided between the private and professional, both with the individuals' interests in mind but also the employers.

Another aspect that can be considered from this study is that the digital native already perceives to have a good understanding of threats stemming from much experience with the digital environment. This could be utilized by employers by translating preferable already existing behaviors from the general digital context into the mobile phone environment. What is important here, and not represented in the data, is to have transparent communication with the digital natives and make sure that their experience and knowledge are translated into the mobile phone environment.

The results provided in this study could act as a aspect to take into account when trying to govern and manage mobile devices when digital natives are a part of an organization. As this group are growing, this perspective will be important to have in mind. Individuals trying to govern mobile phone usage in a company setting should avoid using fear appeals and instead try to find solutions which are secure but at the same time perceived as convionient to the digital natives.

5.6 Study Limitations

Three main limitations need to be considered when viewing the results of this study. The first is the nature of the demographic. This study has only used respondents from Sweden employed by a company providing software or data or software consultancy services. This means that the results are stemming from a social reality described by individuals working in a specific area, constrained by both which nation they are working in and the business area in which their employers are active. The results could be different if either the industry or the targeted country were to be changed.

The second limitation to the study is that fear appeals have been studied by applying a specific model. As described in section 3.2.2 the selected model has been chosen as previous research indicates that the PMT model is currently the most suitable model to study fear appeals in information security, but another theory, for example, technology threat avoidance theory, could be used on the same problem and possibly yield different results. The choice for using PMT is however introduced in section 1.1. PMT is a more mature model according to Boss et al. (2015) and is more rigorously tested than for example FAM and TTAT, which they argue don't have the proper metrics for comparing them to PMT. The argument for using the PMT model is thus that it is more mature, enabling the possibility to rely on the model's functionality compared to if another model were to be used that doesn't have been tested in an equally rigorous way. As the motivation behind this study was to evaluate the effect of fear appeals on digital natives, not to test the validity of different fear appeal models, the choice

was made to use the model that was considered to be the most mature for testing fear appeals.

This study only views include the perception of digital natives. An argument could be made that a comparison between digital natives and previous generations would be proper. As stated in section 3.4 however the choice was limited to only looking at the digital native's perspective to more accurately reflect that social reality, where including the perspective of previous generations would put a limitation on what level of detail the respondents could provide due to time limitations.

As described in 3.2.2 the first sampling stage did not yield enough respondents in order to reach a desired level of saturation. The first stage did only use the purposive sampling approach to find respondents. As saturation did not meet the desired level, the choice was made to change the method for finding respondents during the second and third stages of sampling. In these stages, potential respondents previously known to the author were contacted. These individuals adhere to the previous criteria set for what respondents needed to full fill, enabling the possibility to compare the results from the interviews from the different sampling stages. These two stages did utilize purposive sampling as the same criteria were needed to be adhered to but also convenience sampling as these respondents were easily accessible to the author. Farrugia (2019) describes convenience sampling to yield potential poor quality in the data gathered. Because of the potential drawbacks of convenience sampling, the same criteria for the respondents' characteristics (detailed in 3.2.2) applied in the first sampling stage were applied in stage two and three to combat these potential drawbacks. Still, the two separate approaches for reaching out to potential respondents need to be considered as a limitation for this study as the respondents were gathered in two different ways.

6 Conclusion

The objective addressed in this work was to understand how digital natives can be affected by fear appeals to influence their usage of their phones, and introduced two questions:

1. How does fear affect digital natives in complying with policies regarding private devices?

2. In what way do the different aspects of PMT affect digital natives' usage of mobile phones?

Fear was not found as an emotion that has an impact on the intended behavior of the digital native when using their mobile phone. Although other emotions can be experienced when facing what is perceived as a threat, fear is not one of them. Policies specifically targeting private devices or mobile phones were not in use according to the respondents, although policies that could apply to private devices were present. This did however force the respondents to partake in interpretation regarding what policies should apply to their usage.

How convenient the mobile phone was to use was found to have a large impact on the respondents. This aspect was found in both intrinsic and extrinsic rewards perceived as a benefit for both themselves and their employers. Both threat vulnerability and threat severity had an impact on how the respondents used their phones but not by eliciting any emotion of fear, but rather as a habit or logical response based on previous experiences. The respondents expressed that there are certain things one does not do in a digital environment, all with the same perception of what those things were. Self-efficacies were stemming from the experience of digital environments and were carried over from a computer environment to a mobile phone environment. How convenient a response was to use for the respondents had a big impact on how the response cost was perceived, becoming situational of the respondent's perception of convenience.

As a final conclusion, the digital native does not express that they are influenced by fear in their decision-making regarding the compliance of policies regarding the mobile phone environment or in their usage of mobile phones.

6.1 Future Work

The counterpart to the digital native was disregarded in this study, only managing to provide a perspective from the digital native. Thus, the non-digital natives could be examined with the same study and similar demographic (except for age) to determine what patterns are found in this group. Furthermore, a comparison between the digital native and non-digital native could also be conducted in order to deepening the understanding of the subject.

It was recognized that fear was not experienced by the digital natives but rather other feelings in relation to incidents and threats. Looking into how other feelings impact the digital native's security behavior could bring a more complete picture of how emotions can be utilized to bolster secure behavior.

As this study was carried out in a specific country, perspectives not originating in Sweden could be another interesting path to take. As Ameen et al. (2020) point out, behavior measured by PMT can vary between different countries.

What can be expanded on further is what kind of organizations respondents are deriving from. As explained in 3.2.2 a set of criteria for what kind of companies were considered to find respondents from. All of the respondents in this study were employed by private companies and thus employees from other types of organizations e.g., government bodies etc., could be the target for further research. Even in the private sector, the social realities perceived by respondents from other areas or industries could also be another route to explore further.

What was apparent from the results is that the respondents had a varied perception of whether policies regarding information and cyber security were in place and especially if there were policies for mobile devices and mobile phones. This could further be expanded on in two ways. Either by explicitly targeting respondents from organizations that have information and security policies in place or by targeting organizations that communicate that they have policies that target mobile devices or mobile phones specifically.

Overall, more research into the utilization of security measures by organizations targeting mobile devices and how well it works is a general direction that needs to be expanded on further.

The last thing that became apparent in this study is what can be perceived as the issue of experience when talking about digital natives. Digital natives are experienced with the use of digital environments. The question is if this is an effect of their relatively young age or is this an effect of at which stage of their life, they got access to digital technology. This is a matter that could be explored in more depth.

References

Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, *104*, 106184. https://doi.org/10.1016/j.chb.2019.106184

Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002

Bennett, S., Maton, K., & Kervin, L. (2008). The 'digital natives' debate: A critical review of the evidence. *British Journal of Educational Technology*, *39*(5), 775–786. https://doi.org/10.1111/j.1467-8535.2007.00793.x

Boss, S. R., Galletta, D. F., Benjamin Lowry, P., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly*, *39*(4), 837–864.

Braa, K., & Vidgen, R. (1999). Interpretation, intervention, and reduction in the organizational laboratory: A framework for in-context information system research. *Accounting, Management and Information Technologies*, *9*(1), 25–47.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brodin, M. (2016). BYOD vs. CYOD: What is the difference? *Proceedings of the 9th IADIS International Conference*, 55–62. SwePub.

Bryman, A., & Bell, E. (2013). *F??retagsekonomiska forskningsmetoder*. Liber.

Connaway, L. S., Dickey, T. J., & Radford, M. L. (2011). "If it is too inconvenient I'm not going after it:" Convenience as a critical factor in information-seeking behaviors. *Library & Information Science Research*, *33*(3), 179–190. https://doi.org/10.1016/j.lisr.2010.12.002

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

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

Dupuis, M., & Renaud, K. (2021). Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology*, *23*(3), 265–284. https://doi.org/10.1007/s10676-020-09560-0

Ellersgaard, C. H., Ditlevsen, K., & Larsen, A. G. (2021). Say my name? Anonymity or not in elite interviewing. *International Journal of Social Research Methodology*, 1–14. https://doi.org/10.1080/13645579.2021.1932717

Farrugia, B. (2019). WASP (Write a Scientific Paper): Sampling in qualitative research. *Early Human Development*, *133*, 69–71. https://doi.org/10.1016/j.earlhumdev.2019.03.016

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. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Gill, S. L. (2020). Qualitative Sampling Methods. *Journal of Human Lactation*, *36*(4), 579–581. https://doi.org/10.1177/0890334420949218

Gkioulos, V., Wangen, G., & Katsikas, S. (2017). User Modelling Validation over the Security Awareness of Digital Natives. *Future Internet*, *9*(3), 32. https://doi.org/10.3390/fi9030032

Gkioulos, V., Wangen, G., Katsikas, S., Kavallieratos, G., & Kotzanikolaou, P. (2017). Security Awareness of the Digital Natives. *Information*, *8*(2), 42. https://doi.org/10.3390/info8020042

Helsper, E. J., & Eynon, R. (2010). Digital natives: Where is the evidence? *British Educational Research Journal*, *36*(3), 503–520. https://doi.org/10.1080/01411920902989227

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, 35–49. https://doi.org/10.1016/j.pmcj.2016.06.007

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ismail, K. A., Singh, M. M., Mustaffa, N., Keikhosrokiani, P., & Zulkefli, Z. (2017). Security Strategies for Hindering Watering Hole Cyber Crime Attack. *Procedia Computer Science*, *124*, 656–663. https://doi.org/10.1016/j.procs.2017.12.202

Jarrahi, M. H., Crowston, K., Bondar, K., & Katzy, B. (2017). A pragmatic approach to managing enterprise IT infrastructures in the era of consumerization and individualization of IT. *International Journal of Information Management*, *37*(6), 566–575. https://doi.org/10.1016/j.ijinfomgt.2017.05.016

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-A7.

Jones, C., Ramanau, R., Cross, S., & Healing, G. (2010). Net generation or Digital Natives: Is there a distinct new generation entering university? *Computers & Education*, *54*(3), 722–732. https://doi.org/10.1016/j.compedu.2009.09.022

Kerr, D., & Koch, C. (2014). A Creative and Useful Tension? Large Companies Using "Bring Your Own Device". In B. Bergvall-Kåreborn & P. A. Nielsen (Eds.), *Creating Value for All Through IT* (Vol. 429, pp. 166–178). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-43459-8_11

Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. *Medical Teacher*, *42*(8), 846–854. https://doi.org/10.1080/0142159X.2020.1755030

Krašna, M., & Bratina, T. (2011). The perception of digital security among digital natives. *2011 Proceedings of the 34th International Convention MIPRO*, 1245–1250.

Lee, A. S. (1991). Integrating positivist and interpretive approaches to organizational research. *Organization Sience*, *2*(4), 342–365.

Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*, *33*(2), 250–257. https://doi.org/10.1016/j.giq.2016.01.012

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165. https://doi.org/10.1016/j.chbr.2021.100165

McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security*, *112*, 102526. https://doi.org/10.1016/j.cose.2021.102526

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods*, *1*(2).

Ostermann, U., & Wiewiorra, L. (2017). Raising the Bar The Effect of New and More Appealing Alternatives on User Satisfaction with Incumbent Information Systems. *PACIS 2017 Proceedings*. https://aisel.aisnet.org/pacis2017/128

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon*, *9*(5), 1–6. https://doi.org/10.1108/10748120110424816

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping With a Health Threat. *Journal of Personality and Social Psychology*, *52*(3), 596–604.

Roberts, G., & Rahman, S. (2021). Does Digital Native Status Impact End-User Antivirus Usage? *International Journal of Computer Networks & Communications*, *13*(2), 121–142. https://doi.org/10.5121/ijcnc.2021.13207

Ruiter, R. A. C., Kessels, L. T. E., Peters, G. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, *49*(2), 63–70. https://doi.org/10.1002/ijop.12042

Samarathunge, R. D. S. P., Perera, W. P. P., Ranasinghe, R. A. N. I., Kahaduwa, K. K. U. S., Senarathne, A. N., & Abeywardena, K. Y. (2018). Intelligent Enterprise Security Enhanced COPE (Intelligent ESECOPE). *2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS)*, 1–6. https://doi.org/10.1109/ICIAFS.2018.8913361

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2017). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Shirish, A., Boughzala, I., & Srivastava, S. C. (2016). Adaptive use of social networking applications in contemporary organizations: Examining the motivations of Gen Y cohorts. *International Journal of Information Management*, *36*(6), 1111–1123. https://doi.org/10.1016/j.ijinfomgt.2016.04.002

Siddiquie, K., Shafqat, N., Masood, A., Abbas, H., & Shahid, W. bin. (2020). Profiling Vulnerabilities Threatening Dual Persona in Android Framework. *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)*, 1–6. https://doi.org/10.1109/AECT47998.2020.9194151

Statista. (2021a). *Forecast number of mobile users worldwide 2020-2025*. Statista. Retrieved from: https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/ [2022-01-23]

Statista. (2021b). *Number of private mobile subscriptions in Sweden from 2008 to 2020*. Statista. Retrieved from: https://www.statista.com/statistics/553448/sweden-number-of-private-mobile-subscriptions/ [2022-03-28]

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391. https://doi.org/10.1016/j.cose.2017.07.003

Till, S., & Densmore, M. (2019). A Characterization of Digital Native Approaches To Mobile Privacy and Security. *Proceedings of the South African Institute of Computer Scientists and Information Technologists 2019 on ZZZ - SAICSIT '19*, 1–9. https://doi.org/10.1145/3351108.3351131

Twenge, J. M., & Campbell, S. M. (2008). Generational differences in psychological traits and their impact on the workplace. *Journal of Managerial Psychology*, *23*(8), 862–877. https://doi.org/10.1108/02683940810904367

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, *106*, 102309. https://doi.org/10.1016/j.cose.2021.102309

Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems*, *17*(3), 194–215. https://doi.org/10.17705/1jais.00424

Weeger, A., Wang, X., Gewald, H., Raisinghani, M., Sanchez, O., Grant, G., & Pittayachawan, S. (2020). Determinants of Intention to Participate in Corporate BYOD-Programs: The Case of Digital Natives. *Information Systems Frontiers*, *22*(1), 203–219. https://doi.org/10.1007/s10796-018-9857-4

Appendix 1 – Interview Protocol in English

English version

Good day! First and foremost, thank you for your time for this interview. How has the day been going so far?

My name is Jonathan and I will be conducting this interview with you. This interview is conducted in a study that will be the basis for my master thesis.

Today we will talk a bit about how you use your phone in your workplace and why you choose to use it in this way. The interview will take about x minutes. I will of course not use your name or the name of your workplace in the thesis. The recording of this interview will be used solely for transcription purposes.

Question	Motivation	Follow Up
What are you working with?	Build rapport with respondent	And how long have you been at your current position?
Can you introduce your self?		
Please tell me what mobile devices you are using.	Determine how the device environment of the respondent is currently shaped	Why have chosen to have it this way?
Can you tell me about how your IT environment for professional tasks is set up?	Determine how the device environment of the respondent is currently shaped	
Please tell me about your professional interactions with your mobile phone/phones during a normal day?	Determine if the respondents actions can pose harm for the company. Narcissistic traits (Weeger et al. 2020, Twenage(2008))	What interaction do you choose to do on what device? Why do you choose to carry out these actions on this device?
Please tell me about your personal interactions with your mobile phone/phones during a normal day?	Narcissistic traits (Weeger et al. 2020, Twenage(2008))	What interaction do you choose to do on what device? Why do you choose to carry out these actions on this device?

Is there any pros and/ or cons to using your private phone in your work?	Narcissistic traits (Weeger et al. 2020, Twenage(2008))	
Is there any pros and/ or cons to using your work phone privately?	Narcissistic traits (Weeger et al. 2020, Twenage(2008))	
Can you tell me about an event/ access to information that has shaped how you use your phone?	Understand in what context the respondent (currently) are most likely to be affected by stimuli related to mobile device usage. Thompson et al.(2017)	In what context did this happen?
Can you tell me about how regulations/policies set up by your company have shaped your usage of your mobile phone/phones?	Determine if the respondents have been exposed to fear appeals and the impact of these. (Current Company) Johnston et al. 2016	What are these regulations/policies? Have this affected your behaviour with your phone?
Please tell me about how training you have been exposed to provided by your company has shaped your usage of your mobile phone/phones?	Determine if the respondents have been exposed to fear appeals and the impact of these. (Previous or current company) Johnston et al. 2016	What elements did this training include? Was it any certain part that did affect you? Have this affected your behaviour with your phone?
How have any influence(e.g. comercial, information, personal interaction etc.) in your private life shaped how you use your phone?	Influence of fear appeal on digital natives in a private context(Roberts and rahman 2021)	Did you experience any particular feeling in this case?
What aspects make you change how you use your mobile phone/phones? (How easy it is to use, new ways to use it, threats etc.)	Investigate susceptibility different aspects of PMT, Floyd et al. 2000	
What do you know about threats that can target mobile phones?	Awareness of threats, necessary in order to	Have this affected your behaviour with your phone?

	use fear appeals, Floyd et al. 2000	
How do you perceive the security of a mobile phone in contrast to a computer?	Awareness of threats, necessary in order to use fear appeals, Floyd et al. 2000	Have this affected your behaviour with your phone?
How does your knowledge of threats towards mobile phones impact how you use these phone/phones?	Threat severity Threat vulnerability, Floyd et al. 2000	Have this affected your behaviour with your phone?
If you were to perceive a cyberthreat targeting your phone, how would you proceed to solve the situation?	Examine self efficacy and response efficacy, Floyd et al (2000)	Why is that? Have this affected your behaviour with your phone?
Can you give an example of security mesures that can be used on a mobile phone?	Awareness of self efficacy and power of response efficacy Floyd et al. (2000)	Have used any of these? Which ones? Why? Have this affected your behaviour with your phone?
How do you perceive that new technological solutions is being adopted into the organization you work at? I.e, through employees or from management?	IT Consumerization	Do you have any examples of this?
Do you consider to change your phone behaviours?		

That was all! Have I missed something?

I must thank you once again for your participation in this study, and hope that the rest of your day will be wonderful.

If you have any questions you can just email me.

Appendix 2 – Interview Protocol in Swedish

Svensk version

Goddag! Först och främst tack för att du tar dig tiden och ställer upp på denna intervju. Hur har dagen/helgen varit hittills?

Introduktion av mig. Anledningen till att jag genomför denna intervju.

Vi kommer prata lite om hur du använder din telefon och varför du väljer att använda den på detta sätt. Intervjun kommer att ta ca 60 minuter. Är det så att du vill vara anonym? Vidare kommer det vara så att om du och alla andra deltagare är okej med att inte vara anonyma så kommer jag eventuellt att inkludera lite mer detaljer, men om en av alla som är med och blir intervjuade så kommer alla att förbli anonyma.

Som jag skrev i mailet kommer jag att behöva spela in intervjun, det är du med på?

Vissa frågor skulle kunna upplevas som repetitiva, men de har lite olika funktion så svara bara bra du kan på varje fråga.

Mic test

Är du redo så startar jag inspelningen och så kör vi igång helt enkelt!

Question	Motivation	Follow Up
Vad jobbar du med?	Build rapport with respondent	Hur länge har du varit på din nuvarande position?
Kan du berätta lite snabbt vem du är?		
Kan du berätta vilka mobila enheter du använder idag?	Determine how the device environment of the respondent is currently shaped	Hur kommer det sig att du har valt att ha det på detta sättet?
Kan du berätta lite om din IT miljö i jobbet ser ut?	Determine how the device environment of the respondent is currently shaped	
Vad har du för jobbrelaterade interaktioner med din din mobiltelefon/ dina mobiltelefoner?	Narcissistic traits (Weeger et al. 2020, Twenage(2008))	Vilka interaktioner väljer du att göra på vilken enhet? Varför

		väljer du att göra just dessa saker på denna enhet?
Kan du berätta lite om vilka privata interaktioner du har med din telefon under en normal dag?	Narcissistic traits (Weeger et al. 2020, Twenage(2008))	Vilka interaktioner väljer du att göra på vilken enhet? Varför väljer du att göra just dessa saker på denna enhet?
Finns det några för eller nackdelar med att göra jobbärenden på din privata telefon?	Narcissistic traits (Weeger et al. 2020, Twenage(2008))	Har detta påverkat ditt beteende med din telefon?
Finns det några för eller nackdelar med att göra privata ärenden på din jobbtelefon?	Narcissistic traits (Weeger et al. 2020, Twenage(2008))	Har detta påverkat ditt beteende med din telefon?
Kan du berätta om en händelse eller någon tillgång till information som har ändrat hur du använder din telefon?	Understand in what context the respondent (currently) are most likely to be affected by stimuli related to mobile device usage. Thompson et al.(2017)	i vilken kontext hände detta? Upplevde du någon speciell känsla i detta fall?
Kan du berätta om hur regulationer/policys från företaget har format ditt användande av din mobiltelefon/ dina mobiltelefoner?	Determine if the respondents have been exposed to fear appeals and the impact of these. (Current Company) Johnston et al. 2016	Vad är det för regulationer/policys?
Kan du berätta om hur utbildning via företaget har format ditt användande av din mobiltelefon/ dina mobiltelefoner?	Determine if the respondents have been exposed to fear appeals and the impact of these. (Current Company) Johnston et al. 2016	Vad för delar innehöll utbildningen? Var det någon speciell del som påverkade dig?

Hur har någon influens av något slag (reklam, information, Interaktion med någon annan individ) i ditt privatliv påverkat hur du använder din telefon?	Influence of fear appeal on digital natives in a private context(Roberts and rahman 2021)	Upplevde du någon speciell känsla i detta fall?
Vilka aspekter påverkar ditt användande av din mobiltelefon/ dina mobiltelefoner? (ex. hur lätt det är att använda, tillgång till ny funktionalitet, hot mot mobiltelefoner etc.)	Investigate susceptibility different aspects of PMT, Floyd et al. 2000	är detta kopplat till någon speciell känsla?
Vad vet du om hot som kan riktas mot mobiltelefoner?	Awareness of threats, necessary in order to use fear appeals, Floyd et al. 2000	Har detta påverkat ditt beteende med din telefon?
Hur upplever du att säkerheten är på telefoner jämfört med vanliga datorer?	Awareness of threats, necessary in order to use fear appeals, Floyd et al. 2000	Har detta påverkat ditt beteende med din telefon?
Hur påverkar din kunskap om hot mot mobiltelefoner hur du använder dessa?	Threat severity Threat vulnerability, Floyd et al. 2000	Har detta påverkat ditt beteende med din telefon?
Om du skulle komma i kontakt med ett cyberhot som riktas mot din telefon, hur skulle du gå till väga för att lösa situationen?	Examine self efficacy and response efficacy, Floyd et al (2000)	Varför då? Har detta påverkat ditt beteende med din telefon?
Kan du ge exempel på säkerhetsåtgärder som kan användas på en mobiltelefon?	Awareness of self efficacy and power of response efficacy Floyd et al. (2000)	Har du använt någon av dessa? Vilka? Varför? Har detta påverkat ditt beteende med din telefon?
Hur upplever du att tekniska lösningar börjar användas i ditt företag? E det genom att någon anställd som hittar något nytt eller är det så att ni för lösningar ni skall använda från ledningen?	IT Consumerization	Har du några exempel?

Är du inne på att ändra ditt användande av mobiltelefoner?		

Det var allt! Har jag missat något tycker du?

Jag måste återigen tacka dig så mycket för ditt deltagande och önskar dig en fantastisk fortsatt dag.

Om det är så att du har några frågor är det bara att maila mig.