Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

Eline Hagen Hettervik and Malin Holte

The User Experience of Two-Factor Authentication

Brukeropplevelsen av tofaktorautentisering

Master's thesis in Digital Collaboration
Supervisor: Joakim Klemets
June 2023

NTNU
Norwegian University of
Science and Technology

Eline Hagen Hettervik and Malin Holte

The User Experience of Two-Factor Authentication

Brukeropplevelsen av tofaktorautentisering

Master's thesis in Digital Collaboration
Supervisor: Joakim Klemets
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Abstract

The increased use of digital collaboration tools in organizations has made businesses more vulnerable to cyber threats, making it essential to adopt more secure solutions to protect assets. Human error is a major cause of security breaches, emphasizing the need for secure systems that prioritize usability. Two-factor authentication (2FA) is a particularly challenging security measure as it is such a prominent and frequent part of the user's work process, and can in turn affect routines, habits and thought processes. Therefore, it is important to investigate how employees experience two-factor authentication to understand its impact on security awareness and culture.

This thesis focuses on the user experience of two-factor authentication for employees at an IT company, Atea, using both quantitative and qualitative research methods. The study reveals that frequent authentication requests, unnecessary requests, and technical errors are the most common challenges encountered. Meanwhile, fostering a good cybersecurity culture can enhance the user experience. The thesis also shows how a positive culture can include both individual employee competencies and qualities, and also shared values and trust within the relationship between colleagues and the organization.

Despite the challenges, employees are mostly satisfied with using two-factor authentication, primarily because they understand its benefits. This indicates that increased awareness of the importance of the interdependence between user experience and security measures can lead to better technical solutions in the future. This includes cybersecurity mechanisms that are seamless, usable, effective, and secure, creating value for businesses and society while promoting a positive culture and awareness for cybersecurity.

Sammendrag

Virksomheters økte bruk av digitale samarbeidsverktøy har gjort dem mer sårbare for cybertrusler. Det er derfor viktig å ta i bruk flere og sikrere løsninger for å beskytte ressurser. Menneskelige feil er en betydelig årsak til sikkerhetsbrudd, og understreker behovet for sikkerhetssystemer som prioriterer brukervennlighet. Tofaktorautentisering (2FA) er en spesielt utfordrende sikkerhetsmekanisme, da den utgjør en så fremtredende og hyppig del av brukerens arbeidsprosess, og kan dermed påvirke rutiner, vaner og tenkemåter. Det er derfor viktig å undersøke ansattes brukeropplevelse av tofaktorautentisering, for å forstå dens innvirkning på sikkerhetsbevissthet og -kultur.

Denne masteroppgaven setter søkelys på brukeropplevelsen av tofaktorautentisering for ansatte i et IT-selskap, Atea, ved bruk av både kvantitative og kvalitative forskningsmetoder. Studien viser at hyppige autentiseringsforespørsler, unødvendige forespørsler og tekniske feil er de vanligste utfordringene som oppstår. Samtidig kan utvikling av en god IT-sikkerhetskultur forbedre brukeropplevelsen. Avhandlingen viser også hvordan en positiv IT-sikkerhetskultur kan inkludere både ansattes individuelle kompetanse og kvaliteter, samt felles verdier og tillit i forholdet mellom kolleger og organisasjonen.

Til tross for utfordringene er de ansatte stort sett fornøyde med å bruke tofaktorautentisering, hovedsakelig fordi de forstår fordelene det medfører. Dette indikerer at økt bevissthet om viktigheten av samspillet mellom brukeropplevelse og sikkerhetsmetoder kan føre til bedre fremtidige tekniske løsninger. Dette inkluderer IT-sikkerhetsmekanismer som er sømløse, brukervennlige, effektive og sikre, og som skaper verdi for virksomheter og samfunn, samtidig som de fremmer en positiv kultur og bevissthet rundt IT-sikkerhet.

Preface

This master thesis is written with the Institute of Computer Science and Informatics at Norwegian University of Science and Technology (NTNU) in the spring of 2023. The thesis is the last part of the master's degree in Digital Collaboration and has been written in cooperation with Atea, Trondheim.

In this thesis our goal was to analyze the user experience of two-factor authentication among employees of Atea. We also wanted to discover what could be done to encourage the employees in using two-factor authentication and have a positive experience of it as a security measure. This area of knowledge has appealed to us, and we have gathered knowledge for future careers.

We would like to thank Atea for proposing this exciting case and collaborating with us. We have appreciated getting to know the employees and the company. A special thanks to Terje, our contact person, that has been with us through this whole process. The hospitality has been exceptional from day one.

We would also like to give thanks to Joakim Klemets, our supervisor at NTNU, for professional guidance with all parts of the thesis. All respondents to the survey, the interviewees and all proofreaders also deserve a thank you. This thesis could not have been done without you.

Trondheim, June 2023

Eline Hagen Hettervik and Malin Holte

Table of Contents

Figure overview

Table overview

Abbreviations

2FA	Two-Factor Authentication
ADFS	Active Directory Federation Services
E3	Enterprise 3
E5	Enterprise 5
FIDO	Fast Identity Online
IRT	Incident Response Team
IT	Information Technology
M365	Microsoft 365
MFA	Multi-Factor Authentication
NSD	Norsk Senter for Forskningsdata
SFA	Single-Factor Authentication
Sikt	Norwegian Agency for Shared Services in Education and Research
SSO	Single Sign-On
TSD	Service for Sensitive Data
UX	User Experience
VPN	Virtual Private Network

1 Introduction and Background

The rapid technological development in society and the digital transformations of organizations have led to new, and constantly evolving, needs and wants for businesses and their employees. As work processes are increasingly digitized and employees and their digital tools become interdependent in their everyday work life, one also becomes more vulnerable for cyber threats, simultaneously as the scope of cyber attacks increases (Alsharif et al., 2022; Boehm et al., 2020; World Economic Forum, 2022). With the large amount of money being invested in the digital workplace, and the potential financial losses at risk if cybersecurity is not realized, it is crucial and urgent that businesses address these issues.

The field of usable security has over the last 25 years established a large body of research that raises awareness of the relationship between cybersecurity and human factors (Lennartsson et al., 2021; Theofanos, 2020). The specific empirical problem that forms the basis for our research question, is the observation that users of digital collaboration tools often experience integrated, interactive cybersecurity measures as a hindrance for efficiency and disturbance for agility in work processes. Firstly, this is frustrating and dissatisfying for the user, contributing to a negative user experience. Secondly, the risk of users obtaining a negative attitude toward security measures exists, as these experiences become a part of their everyday work life. Furthermore, as security measures are increasingly being implemented in technological solutions, and become automated actions by the user, it may lead to a lack of critical thinking and awareness regarding the meaning and value of security measures. If the choice whether to use a security mechanism is given to the user, it could potentially lead to users simply avoiding or circumventing the efforts for enhanced security.

With our research problem we aim to explore these empirical issues on how security measures are experienced by the users of digital collaboration tools. Specifically, we want to use two-factor authentication in Microsoft 365 as our case, because of its widespread adoption by enterprises. By researching this issue, one might further discover how security measures can become a seamless part of digital collaboration tools, while still fostering a good culture and awareness for cybersecurity.

Usable security is an interesting and timely topic because both security and user experience are important, and yet often seen as competing aspects of the collaborative IT solutions in today's businesses. Balancing these factors are critical to the success and popularity of collaborative tools in organizational settings (Tolone et al., 2005). Interestingly, these considerations and efforts take place within a larger organizational cybersecurity culture, which is argued to be a direct reflection of the information system user’s behavior (Glaspie & Karwowski, 2018).

Additionally, the pandemic has led to new ways of working, particularly working from home. This has further digitized collaborative work, as well as increased general cybercrime, which has somewhat altered the context of the issue at hand (Georgiadou et al., 2022). Organizations' increasing use of cloud-based collaboration tools has overall increased the scope of the problems that relate to security, compliance, cost and integration (Violino, 2020).

A negative cybersecurity culture can contribute to vulnerabilities in the whole organization, and security interruptions come with many repercussions (ENISA, 2017). The possible worst-case outcomes if security is not handled correctly or as intended, or in itself is not sufficient, cannot be underestimated. It can result in a great financial loss for businesses (Malmedal & Røislien, 2016), but it can also mean lost trust and integrity, both from internal and external interests (ENISA, 2017). Our motivation for this research problem is therefore the opportunities that lie in understanding and documenting these issues, so that organizations can take steps to improve their cybersecurity culture.

Over the last two decades, human errors have been the leading cause of security incidents (Evans et al., 2019; Kirlappos & Sasse, 2014; Mancuso et al., 2014; Triplett, 2022). In fact, Schneier (2015) described people as the weakest link in the security chain. This may be partly because users' values and needs are not sufficiently addressed in technological solutions, as even interactive technology often follows a systems design approach that focuses on the components, rather than the users. This will have implications on security usability (Fassl et al., 2021), meaning that users will not interact with security measures as intended. In the development of high-quality digital tools, the users cannot be isolated from the technology (Malmedal & Røislien, 2016). This thesis aims to examine the critical relationship and dependency between cybersecurity culture and user experience.

We have specifically chosen two-factor authentication as the security mechanism in our case for several reasons. Firstly, in collaborative digital tools, two-factor authentication is possibly the most noticeable security mechanism for the user, as it requires the most attention and interaction. Secondly, the layered approach of multi-factor authentication reduces the probability of several unwanted security events (Acemyan et al., 2018). Gunson et al. (2011b) and Marky et al. (2022) state that two-factor authentication significantly mitigates security weaknesses. In fact, a report from Microsoft presented by their director of identity security, Alex Weinert, claims that two-factor authentication can prevent instances of unauthorized access to user accounts by 99.9% (Weinert, 2019). Therefore, two-factor authentication is widely recommended as industry standard. These are noteworthy reasons to also uncover the user experience of two-factor authentication.

Although significant research in recent years shed light on these topics, there are still issues that need to be further examined. Though usable security has generally found some attention in information technology, there has been considerably less attention to digital collaboration tools distinctively (Kocksch et al., 2018). Previous studies might have missed specifically how the users experience the importance of IT security mechanisms (Fassl et al., 2021). We want to uncover the motivations of employees in using security mechanisms like two-factor authentication. Similarly, there is a great deal of literature on organizational cybersecurity culture, but there lack perspectives on how culture and individual user experiences mutually affect each other. Additionally, our case study differs from existing ones by researching an IT company. Further, when the user experience of cybersecurity mechanisms is entirely understood, it is also possible to discover causalities between this and certain behaviors.

1.1 Research Question

Our motivation for this thesis is to explore and map out how users experience two-factor authentication as a security mechanism in routine use of digital collaboration tools. Besides documenting the user experience, we want to bring to light the underlying reasons, the causes, and effects. For instance, if security measures are experienced as cumbersome, what are the alternative responses, and the consequences of these deviations? The purpose of our research is to contribute to the field by laying the ground for developing more favorable solutions where user experience and cybersecurity enhance each other. We also acknowledge that individual user experiences do not occur in isolation, but rather in a shared, organizational culture. Therefore, we seek to examine the interplay between these two phenomena.

Based on the literature, or lack of literature in the specific field, we have defined the following research question:

"How is two-factor authentication as a security mechanism experienced by users in Microsoft 365?"

To be able to provide an elaborate answer to the main research question, we have designed three sub-research questions that we aim to answer throughout the thesis:

RQ1: What are the challenges in two-factor authentication that users experience in Microsoft 365?

RQ2: Why do users experience the described challenges with two-factor authentication in Microsoft 365?

RQ3: How does the user experience of two-factor authentication and the culture for security in an organization affect each other?

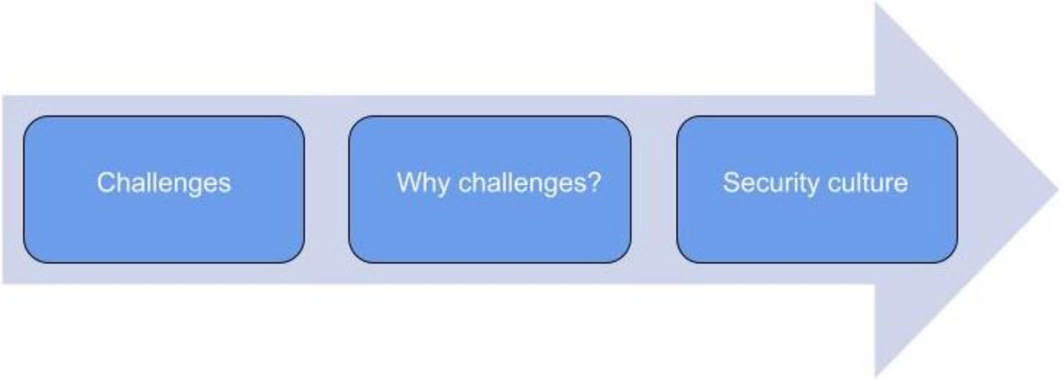


Figure 1.1 The connection between the three different sub-research questions.

The figure presented above (figure 1.1) depicts the connection between the three different sub-research questions over time. The first question aims to uncover the challenges that users experience in Microsoft 365. Identifying the challenges is essential to comprehend how users experience two-factor authentication. The second research question seeks to investigate why the users experience these challenges. If our thesis could further encourage the development of more usable IT solutions, where two-factor authentication is not seen as a barrier, it is necessary to understand the causes of these challenges. The final question aims to understand how the user experience and the culture for security in the organization can affect each other. If a company has a natural good culture for cybersecurity, there is a reason to think that more employees will have a positive attitude toward security measures. This can in turn contribute to a greater overall experience of two-factor, simultaneously as positivity toward security mechanisms can create a satisfactory security culture.

To address the research question, we conducted a survey and interviewed employees at Atea. This IT consultancy firm specializes in cybersecurity and digital collaboration tools, i.e. Microsoft products, among other things. Atea provided us with access to their employees, such as consultants and other in-house employees. These professionals have a great deal of knowledge and a breadth of experience relevant to our research questions, as they are both casual users (that includes employees without specific security expertise), as well as security- or Microsoft 365-experts, that use two-factor authentication at work every day.

2 Theory

In this chapter the theoretical background for the thesis is presented. The theoretical background is constructed on the basis of former studies and literature that is of importance and relevance to our research question. This foundational framework forms the data collection methods and data analysis and supports the arguments and conclusion. The chapter covers four main topics relevant to our research question: cybersecurity, digital collaboration tools, two-factor authentication, and user experience in technology. We define central terms, explain the theoretical landscape and present different views from existing research.

2.1 Cybersecurity

2.1.1 What is Cybersecurity?

Cybersecurity is one of the overall concepts explored in this thesis. Cybersecurity has become increasingly critical to countries, organizations, and internet users, and will continue to be in the future (Bishop, 2003). It is crucial to define and understand cybersecurity and what requirements to meet because different organizations have different perspectives on cybersecurity. Bishop (2003) defines a system's security as a specific statement of what is and is not allowed. Put another way; if a system is non-secure, a user can successfully execute a disallowed action. On the contrary, if a system is secure, users can only perform actions that are allowed. Security mechanisms have the goal of ensuring that systems never enter disallowed states, and they must be configured correctly so they do not fail their intended task.

The terms cybersecurity and information security are often used interchangeably, and though the concepts are related, they are not totally equivalent. Figure 2.1 shows a fundamental difference, namely how information security goes beyond the boundaries of cybersecurity. Information security involves security of information, regardless of realms, while cybersecurity involves specifically everything security related in the cyber realm (Taherdoost, 2022; von Solms & van Niekerk, 2013). Besides drawing this line, several different definitions of the two terms exist. Taherdoost (2022) refers to ISO/IEC 27032:2012 and ISACA CSx Cybersecurity Fundamentals Study Guide as reputable sources, defining cybersecurity as the "preservation of the confidentiality, integrity, and availability of information in Cyberspace" (p. 484), and information security as the "preservation of the confidentiality, integrity, and availability of information" (p. 484). As seen from these definitions, both can be relevant to the access control of information, however two-factor authentication for digital collaboration tools (see section 2.3 and 2.2. respectively) are necessarily a mechanism for the digital environment. With this in mind, our thesis will target cybersecurity (also referred to as IT security), but both terms will be used in the following text according to these definitions.

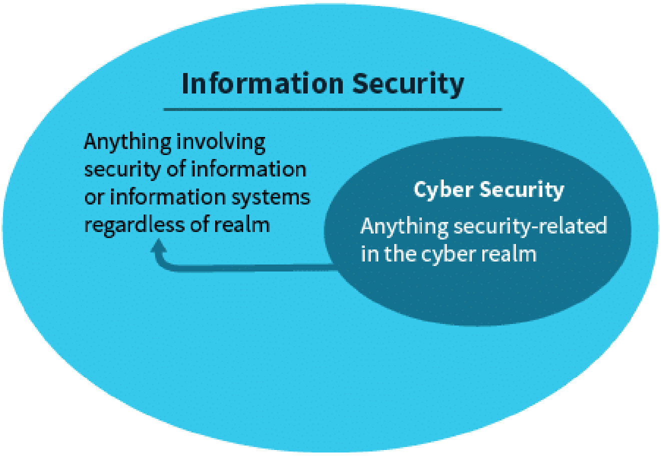

Information Security
Anything involving security of information or information systems regardless of realm
Cyber Security
Anything security-related in the cyber realm

Figure 2.1 The difference between information security and cybersecurity.

Protecting information systems or sensitive data from cybercriminals is the main objective of cybersecurity (Al Mehairi et al., 2022). To ensure that data is secure, according to Al Mehairi and Rajesh (2022; 2022), one refers to the CIA triad: Confidentiality, Integrity and Availability, as can be seen in figure 2.2. Together, these three related principles guide efforts toward information security. The first principle, confidentiality, ensures that only the right people have access to sensitive data. There are usually some organizational policies on how employees can access data, and the data is meant to be inaccessible for others (Al Mehairi et al., 2022). Some methods to achieve confidentiality are security tokens and authentication, like for instance biometric verification (Rajesh, 2022). We therefore seek to understand the user experience of authentication, in order for the method to later improve and to further ensure that confidentiality is upheld. Integrity, as the second principle, guarantees that information systems are not changed or modified by accident or by external threats. If sensitive data are lost, drastic measures will be taken to recover. The last principle of the CIA triad is availability, which makes certain that end-users have access to available and useful data. The data or information should be available whenever the users require it. Malicious activity and malfunctions should not hinder this availability (Al Mehairi et al., 2022). To reduce downtime of the system and ensure high availability, the system should have a disaster recovery plan (Rajesh, 2022), which is a plan to return to normalcy after a disaster occurred (Ogie et al., 2022).

CONFIDENTIALITY
CIA TRIAD
INTEGRITY
AVAILABILITY

Figure 2.2 The CIA triad to ensure that data is secure.

With today's widespread use of digital collaboration tools, additional and more complex security measures are required to protect the organization and the large number of users working simultaneously in the same system. While fulfilling its purpose as a collaboration tool, it is important that the system is secure, including protection against unauthorized exploitation.

Cybersecurity is a critical issue that requires organizations and people to take careful consideration when discussing steps toward improving security. Companies need security features, but done the right way. If companies and users do not understand security, the attempt of protecting themselves in cyberspace will not succeed (Bishop, 2003). Questions to reflect on to ensure requirements, policy, and mechanisms, respectively, include "what do you expect security to do for you?", "what steps do you take to reach the expectation set above?" and "what tools, procedures, and other ways do you use to ensure that the above steps are followed?". Relating this to organizations, Bishop (2003) wrote:

> If the policy satisfies the requirements, and if the mechanisms enforce the policy, a company that uses a system with many security features, all of them enabled, could in fact be less secure than its competitor, which uses the same system but enables only some security features (p. 69).

Authentication is only a minor area of security, but not an insignificant one, as we will further elaborate on.

2.1.2 Cybersecurity Culture

Understanding the concept of culture is not easy, as there is a lack of consensus among authors on how it is defined. Yet, a widely accepted definition of organizational culture presented by Schein and Schein (2016) is as follows:

> The accumulated shared learning of that group as it solves its problems of external adaptation and internal integration, which has worked well enough to be considered valid, and therefore, to be taught to new members as the correct way to perceive, think and feel in relation to these problems (p. 6).

In addition to this definition, Schein and Schein (2016) present a three-level model of culture, which consists of artifacts and creations, values and beliefs, and basic assumptions. Parsons et al. (2010) explain how these three layers to culture relate to an organization. The first layer, artifacts and creations, are the most visible and apparent layer, they are things that can be seen and heard easily by internal and external actors, like objects, language and habits. The second layer, values and beliefs, guide employee behavior through direction and guidelines provided by senior management. Though, there is no guarantee these will lead to actual, specific employee behavior. The last layer, basic assumptions, are at the core of an organization's culture. Basic assumptions are invisible and elusive assumptions that individual employees hold about the organization and how it relates to its environment and human behavior, making them challenging to comprehend and assess.

Consequently, cybersecurity culture can be defined in equally many ways as culture itself. Based on a literature review study of 50 relevant articles, AlHogail and Mirza (2014) suggest defining information security culture as:

> The collection of perceptions, attitudes, values, assumptions and knowledge that guides how things are done in an organization in order to be consistent with the information security requirements with the aim of protecting the information assets

> and influencing employees' security behavior in a way that preserving the information security becomes a second nature (p. 2).

Similarly to Schein and Schein's (2016) definition of culture, the above definition implies that some internal, individual thought processes result in some collective behavior that is considered as the right way of acting. A cybersecurity culture is an integral part of the extensive organizational culture in any organization, and must not be assessed in isolation (AlHogail & Mirza, 2014; Parsons, 2010).

Besides AlHogail and Mirza's (2014) definition establishing the link between culture and behavior, Sample et al. (2018) put it in other words. They argue that cultural values for information security are crucial for the actual individual behaviors by providing the context for said behavior, thus determining the norm for a group. For instance, Glaspie and Karwowski (2018) agree that employees will adopt the attitudes, opinions and practices of their teams in the absence of expertise. Sample et al. (2018) explain how this correlation arises as cultural beliefs and biases embedded in human thought processes are revealed in thought patterns. When these thought patterns are reinforced, they manifest in behaviors in the digital realm. In return, users' experience and involvement alters users' perceptions and attitudes toward information security (Glaspie & Karwowski, 2018). So though computer systems are standardized, Hofstede et al. (2010) note that how they are used is dependent upon the mind of the user.

Consequently, information security is not purely a technical issue. In fact, many authors claim that humans are the weakest link in information security (Glaspie & Karwowski, 2018; Kirlappos & Sasse, 2014). To combat this, organizations need to prioritize and invest in a positive cybersecurity culture, including both management and employees on all levels (Glaspie & Karwowski, 2018). Cybersecurity training is an effective way to target human factors, as well-informed users of digital tools tend to have a more positive attitude toward cybersecurity, and therefore a more desired behavior, including using the security mechanisms as intended. Organizations that succeed at security policy compliance will strengthen the overall information security posture and minimize the risk posed to information privacy (Glaspie & Karwowski, 2018). These risks include security breaches, loss in external and internal trust and integrity, and ultimately financial loss (Acemyan et al., 2018; Dasgupta et al., 2017; Glaspie & Karwowski, 2018).

2.1.3 Training in Cybersecurity

Numerous authors argue that the human aspect of security is of essence (Bishop, 2003; Parsons, 2010; Sample et al., 2018). Adequate organizational cybersecurity training has the potential to enhance these human factors. This is because users need to have sufficient knowledge and understanding of the security principles for the effort of more secure systems to work as intended. Users need to understand how these principles apply in a given situation, how to define the appropriate requirements and the policy, and ultimately, they need to know how to use the technology to implement the policy.

Employees that lack proper training can make intentional or unintentional errors that pose great security risks for their company (Glaspie & Karwowski, 2018; Parsons, 2010). The training of cybersecurity awareness, knowledge and competencies in an organization need to be sufficient enough to eliminate these errors (Glaspie & Karwowski, 2018). Keeping in mind that two-factor authentication is not purely a technical implementation, but used and handled by employees, it becomes evident that training in two-factor authentication in an organizational setting should also meet these requirements.

To accomplish the above goals, employees in companies need training relevant to their respective roles and responsibilities (Glaspie & Karwowski, 2018). The training should not only result in a specific behavior, but also stimulate individual awareness that fosters a positive culture to reinforce that wanted behavior (Glaspie & Karwowski, 2018). Training programs should benefit employees by promoting the consistent understanding of the importance of acting compliant and avoiding risks (Glaspie & Karwowski, 2018). The content should also be constantly reviewed and updated as the assumptions change.

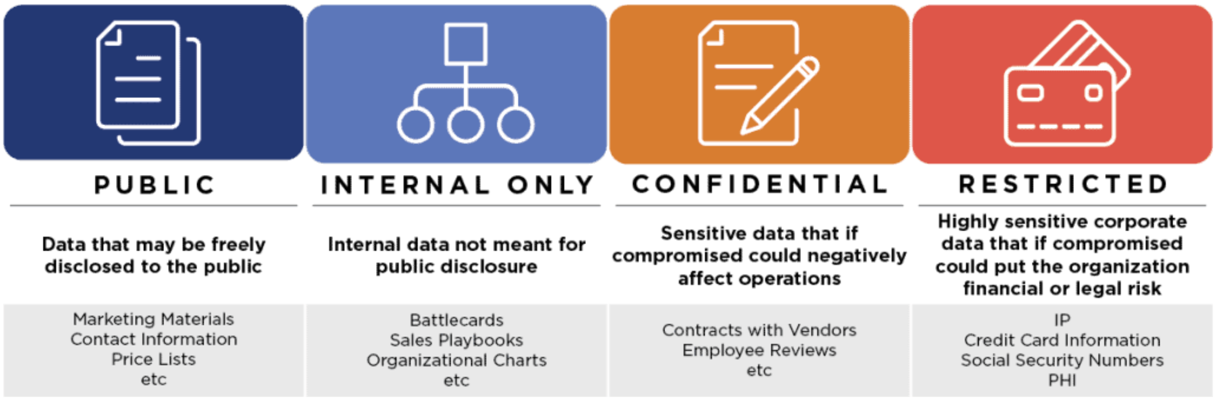
Glaspie and Karwowski (2018) and Parsons (2010) emphasize the importance of training that bridges the gap between the organization's security policies, their business objectives and the needs of the users. The authors argue that the content of the training should not be "technocratic" (meaning that the training fails to meet the users at their level of competencies), but rather focused on the formation of habits in relation to the users' experience and the procedural options available for them. Relevant and immersive training of specific activities, e.g. the impacts of a security incident, are shown to be effective in increasing awareness (Glaspie & Karwowski, 2018). McBride et al. (2012) also stress the importance of training that is relevant to individual user experiences, based on different personality types. The authors' study shows that different personality types react differently to threats and sanctions. Training therefore needs to be tailored and diverse to meet those various personalities.

2.2 Digital Collaboration Tools

Digital collaboration tools define a category of software, developed and used for a specific purpose. In order to understand the context of these tools in the digital age, and accordingly their importance and relevance, one needs to make the distinction between digitization and digitalization. The process of merely replacing a physical object with a digital equivalent is called *digitization*, whereas *digitalization* is the transformation that seeks to generate new sources of value, by placing digital information at the core of the business (Orellana, 2017). Digital tools therefore do not simply digitize business processes, but also deliver unique value to the organization.

Digital collaboration is defined by Salopek (2000) as "the use of technology to enhance and extend the abilities of individuals and organizations to collaborate, independent of their vertical area" (p. 1). Collaboration can actually be improved by the use of digital collaboration tools, according to research (Hilliger et al., 2022; Hmelo-Silver et al., 2013), since digital collaboration tools are tools that facilitate this collaboration. These tools can create new streams of meaningful and significant data, which can be leveraged for digitalization (Orellana, 2017).

When accessing systems and tools, the data are classified based on the content's level of sensitivity. There are four classifications of data; public, internal, confidential and restricted, according to Saini et al. (2022). Figure 2.3 gives a short explanation of the different classifications. Since users collaborate in digital collaboration tools, opposed to digital tools in general, it is imperative that only the right people get access to the right systems and data, even if everyone is working within the same digital tool. Some employees may only be authorized to access confidential information, while others can access restricted information. Two-factor authentication would be the recommended and safest method for the system to verify the users' identities, because of the reasons stated in section 2.3. When employees have proven their identity, the right access will be given to them. In the case of two-factor authentication in digital collaboration tools, it is crucial that the user experience of two-factor authentication is adequately enough for all the system users to understand and use it as intended, individually and collectively.



PUBLIC	INTERNAL ONLY	CONFIDENTIAL	RESTRICTED
Data that may be freely disclosed to the public	Internal data not meant for public disclosure	Sensitive data that if compromised could negatively affect operations	Highly sensitive corporate data that if compromised could put the organization financial or legal risk
Marketing Materials Contact Information Price Lists etc	Battlecards Sales Playbooks Organizational Charts etc	Contracts with Vendors Employee Reviews etc	IP Credit Card Information Social Security Numbers PHI

Figure 2.3 An explanation of the four different data classifications.

Isenberg et al. (2011) categorized collaboration into four types (as can be seen from figure 2.4), which can be called the space/time matrix. The top-left square of the figure represents the face-to-face interactions, where everyone participating in the collaboration is co-located synchronously. This can for instance be meeting rooms and classrooms. The bottom-left square is the continuous tasks that happen in for example team rooms or large public displays - it is co-located, but happens asynchronously. The top-right square represents remote interactions, such as video conferencing, instant messaging etc. that take place simultaneously, but distributed. The bottom-right square portrays a distributed location and asynchronous time, and examples include emails and group calendars. Digital collaboration tools can be used in all four instances, and how Microsoft 365 (M365) is used in teams and organizations is an example of such use. For collaboration to occur at different locations and at different times, digital collaboration tools are essential. For co-located collaboration the tools can still enhance and streamline the collaboration process, improving efficiency and productivity.

There are a number of different commercial actors developing digital collaboration tools. Among the leading ones are Google and Microsoft, which offers complete, enterprise solutions. These are widely used in businesses both in Norway and globally, although several other tools are also used. Even though their applications are integrated differently, they share many common principles. Employees are able to write, chat, talk, video-chat, edit, delete, etc. online and simultaneously, which facilitates effective collaboration. This implies that employees of companies have the possibility of collaborating with colleagues at different locations, among other beneficial functionalities.

Successful adaptation of collaboration tools and collaborating platforms require (similar to other types of software) correct implementation, adoption and maintenance, in addition to maneuvering privacy and security concerns. Orellana (2017) argued that privacy and security were the biggest barriers for these platforms to be fully adopted. During this thesis we will expectantly discover if security measures, specifically two-factor authentication, is such a barrier for M365 as a digital collaboration platform. If the user experience of two-factor authentication turns out to be unsatisfactory (i.e. at Atea), it could imply that other similar companies face the same challenges. This could also make it difficult for organizations to fully adopt two-factor authentication in digital collaboration tools. Failure to adopt two-factor authentication, or employees that do not sufficiently understand two-factor authentication, could result in security breaches.

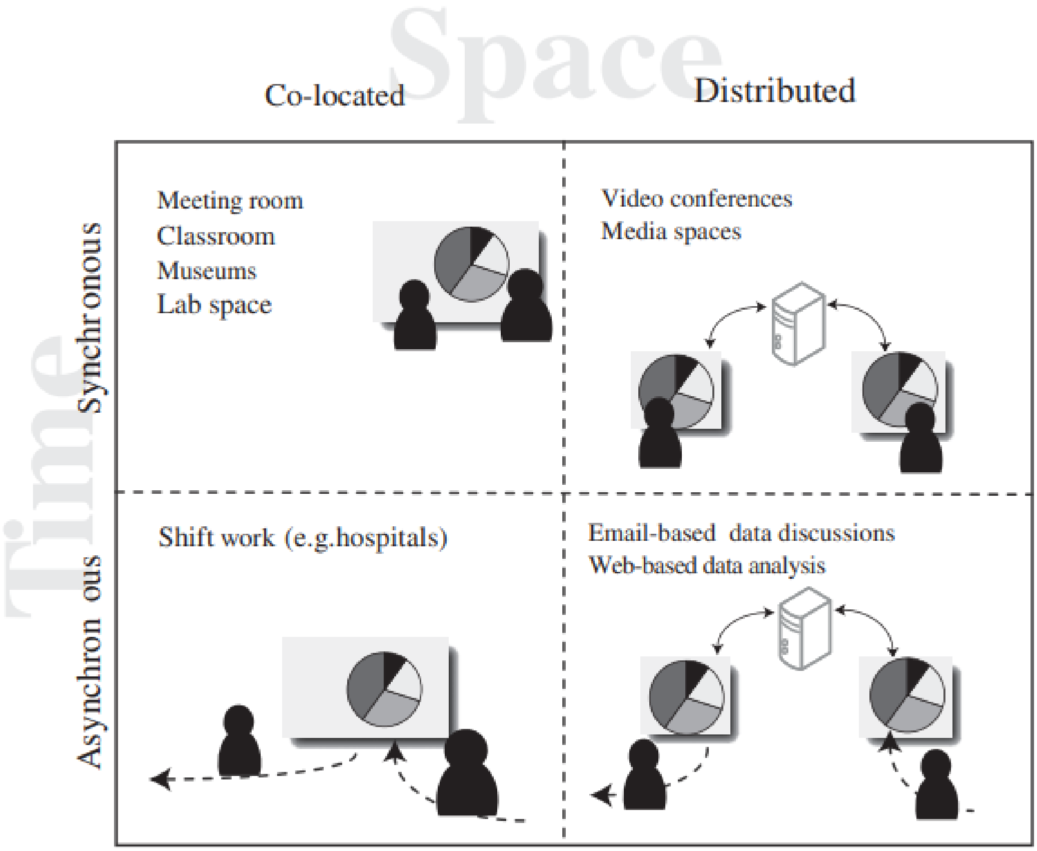


Figure 2.4 Space/time matrix of collaborative work (Isenberg et al., 2011).

2.3 Two-Factor Authentication

2.3.1 Authentication in General

In the field of cybersecurity, different definitions of authentication exist. Simply put, it is the process of validating a user's (or another entity's) identity to access a system (Andress, 2014; Lal et al., 2016; Schneier, 2003). The term authentication is often confused with the terms identification and authorization. The three concepts are related, but have distinct meanings. Identification is to claim an entity's identity, authentication is to prove the claimed identity, while authorization is verifying their access rights (Andress, 2014; Lal et al., 2016; Schneier, 2003). To rephrase, when a user attempts to access some system or information, identification asks; "who are you?", authentication asks; "can you prove who you are?" and authorization asks; "what are you allowed to access?". Together, these three processes provide security and constitute access control for an information system.

2.3.2 Single- and Multi-Factor Authentication

Generally, authentication systems can be grouped into two categories, namely single-factor authentication (SFA) and multi-factor authentication (MFA). Two-factor authentication (2FA) is a subset of MFA, and the most common. The factors referred to in these terms are commonly grouped as following (Gunson et al., 2011a; Marky et al., 2022):

- Something you know (knowledge); some cognitive information, like a password.
- Something you have (possession); some physical token, like a computer or a phone.

- Something you are (inherence); some intrinsic, unalienable and unique feature of the identity of the user, usually biometric features, like fingerprints or facial recognition.

The grouping of authentication factors is visually explained through figure 2.5. Each of the blue circles represent a single-factor authentication; something you know, something you have and something you are. Single-factor authentication is the simplest form of authentication. It only uses one factor to verify a user's identity (Gunson et al., 2011a), and is the most commonly used category of validation, usually in the form of passwords (Andress, 2014). If you combine factors from two or more of the circles (i.e. groups) you get MFA, and if you combine exactly two circles, 2FA is used.

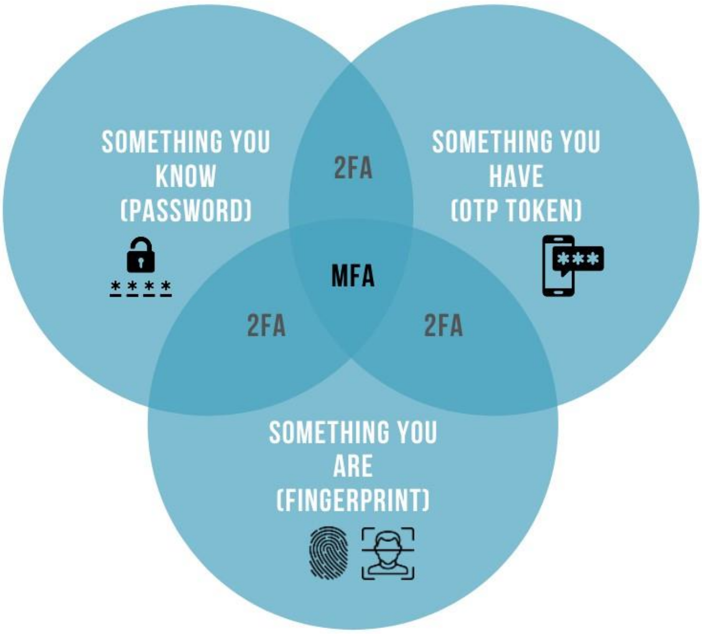

SOMETHING YOU KNOW (PASSWORD)
****
2FA
SOMETHING YOU HAVE (OTP TOKEN)
***
MFA
2FA
2FA
SOMETHING YOU ARE (FINGERPRINT)

Figure 2.5 A visual explanation of single-, two- and multi-factor authentication.

Two-factor authentication is a subset of the broader category for multi-factor authentication. MFA is fundamentally different to SFA by providing a layered approach to securing access to data and applications (Nag et al., 2015), where more than one group of authentication factors is provided from the user. MFA as a practice applies well to the information security strategy called *defense in depth*, which enforces the use of multiple layers through information systems (Nirmal et al., 2022). Accordingly, the layered approach of MFA reduces the probability of several unwanted security events (Acemyan et al., 2018).

2.3.3 Definition of Two-Factor Authentication

2FA requires exactly two groups of factors from the user (Marky et al., 2022). There are no restrictions on which factors one can combine. The different 2FA technologies and factors have different security properties and contribute with different qualities to the authentication process (Acemyan et al., 2018). Combining these factors significantly mitigates security weaknesses (Gunson et al., 2011a; Marky et al., 2022). In fact, a report from Microsoft presented by their director of identity security, Alex Weinert, claims, as mentioned in chapter 1, that 2FA can prevent instances of unauthorized access to user accounts by 99.9% (Weinert, 2019). Nevertheless, one has to be aware that though 2FA may reduce unauthorized access, MFA can also be bypassed (Grimes, 2019).

2FA reduces many of the disadvantages associated with the cybersecurity provided by SFA (Dasgupta et al., 2017). Internet users are known to create weak passwords when allowed, and often use the same password for multiple accounts. This represents a commonly exploited authentication vulnerability by automated attacks (Abbott & Patil, 2020; Stanislav, 2015). Most data breaches involve weak, compromised or default passwords (Dutson et al., 2019). To prevent attacks, login systems can enforce password complexity rules, but research shows that users find it challenging to create, use and remember a strong text based password (Abbott & Patil, 2020; Ur et al., 2015). Even if the password is strong, the user still has a 30% chance of falling for a phishing scam, which is an online scam that targets customers by sending an email that appears to be from a well-known source (Abbott & Patil, 2020). This email asks for personal information, and passwords can easily be stolen. If a password is stolen, MFA can hinder the attacker from getting access to people's personal data. Generally, only enabling SFA is strongly discouraged by experts (Abbott & Patil, 2020).

2.3.4 Two-Factor Authentication in Practice

Over the past ten years the number of online services that provide 2FA for account security to their end-users has steadily increased (Stanislav, 2015), and 2FA's popularity is quickly rising (Acemyan et al., 2018). Today, 2FA is widely recommended across industries (Golla et al., 2021; Marky et al., 2022), but despite this there still exist password-protected systems where 2FA is not available (Acemyan et al., 2018).

There are several examples of commercial MFA- and 2FA solutions (Dasgupta et al., 2017; NSA, 2020). Microsoft's solution for 2FA is one of them, using an app on the smartphone, an SMS or an automated call as the second factor of authentication. Similarly, Google has its own solution, with similar authentication as Microsoft. BankID is a Norwegian solution developed jointly by the banking industry and based on a common infrastructure (Mirkovic, 2010). Another common example is a credit-card (ownership) combined with a PIN (knowledge) for payment (Stanislav, 2015).

Active Directory Federation Services (ADFS) is an example of a service that connects cloud and on-premises identities in a company and is used to authenticate toward services still dependent on local domain servers. If the local domain servers are down - one cannot access all systems and authentication might fail (Grillenmeier, 2021). Compared to other methods for authentication, ADFS is slower.

Fast Identity Online (FIDO) is another way to use MFA, where passwords are eliminated and keys are supported (Zwane et al., 2021). FIDO is a physical registered device that works as the second factor (i.e. token) in the authentication process. An example of a USB-token is shown in figure 2.6. Integrating MFA and FIDO protocol would ensure increased security and ease of use as people nowadays can use their mobile phone as the token.

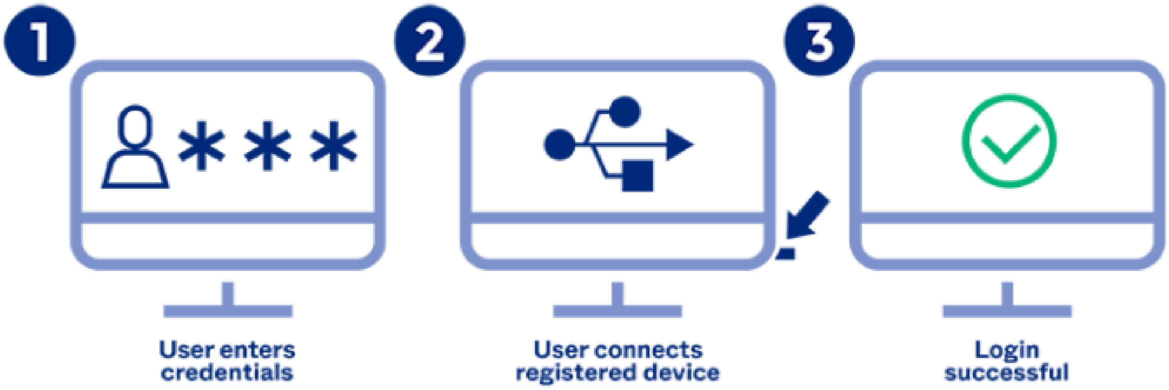


Figure 2.6 An example of FIDO authentication with a USB-device as a token.

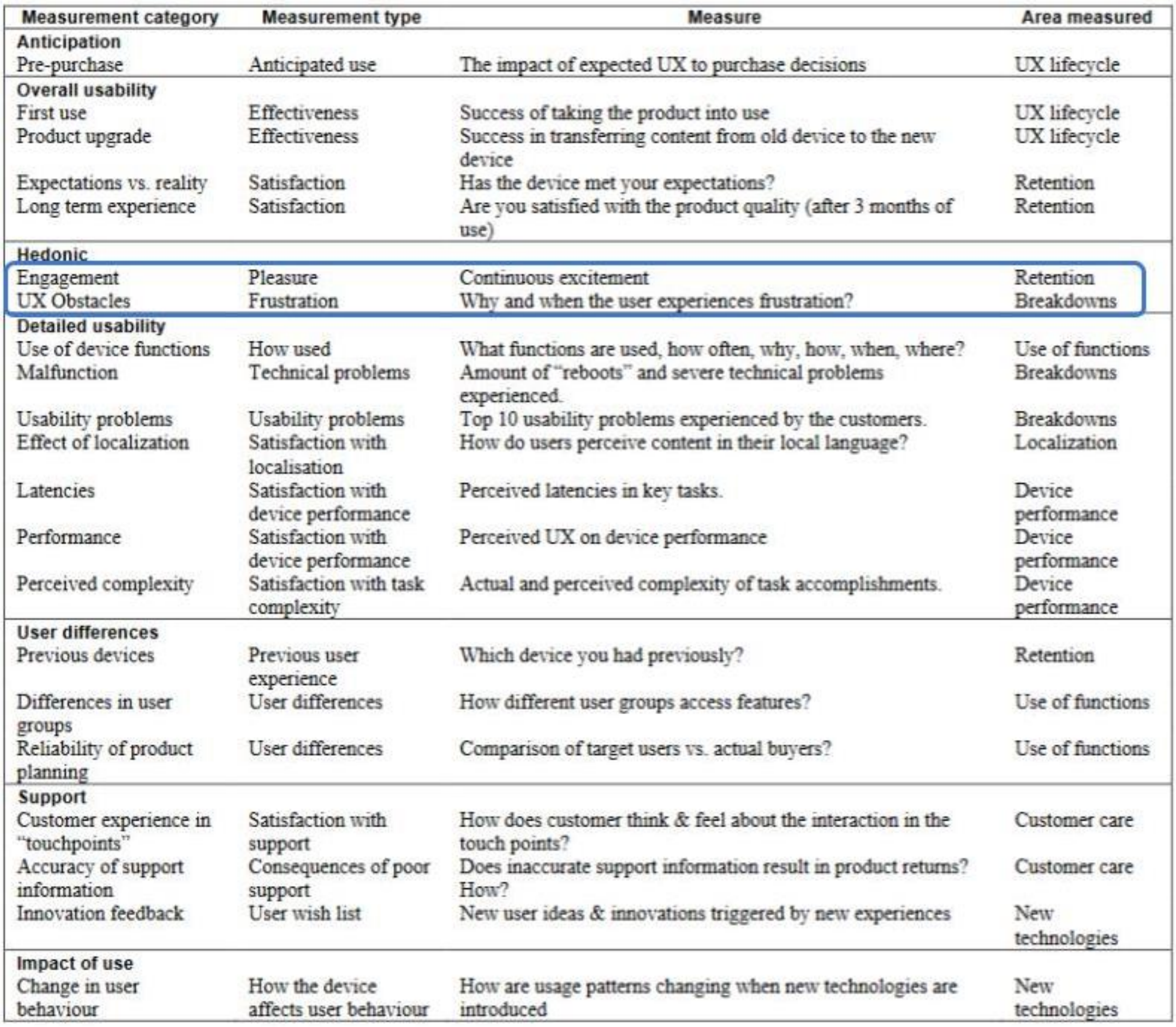
The different MFA-products are often quite similar in many ways, but can also differ in the features and mechanisms being supported, like available platforms, authentication factors, lifecycle support and cost structures (Dasgupta et al., 2017; NSA, 2020).

2.4 User Experience in Technology

2.4.1 Definition of User Experience

In all areas of technology which involve human-computer interaction, the user experience, i.e. UX, is crucial for success. UX is in itself a neutral concept, but positive user experiences are essential to encourage humans to change their habits and behavior in the direction of enhanced security. It is important to note that UX is a broad, all-encompassing and complex term and several definitions are suggested by researchers. Bevan (2009a) defines UX as "a person's perceptions and responses that result from the use and/or anticipated use of a product, system or service" (p. 1). In addition, the related concept of usability is defined by Bevan (2009a) as the "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (p. 1). The central difference between UX and usability is that UX concerns the entire subjective experience of the process of the interaction and the reinforcement of that experience, while usability is an objective and isolated measure of how well goals are achieved. The goal of high quality UX is to optimize the combined UX from the expectation, through the actual interaction and all the way to the reflection on the whole experience.

Both usability and user experience are measured during or after the use of a system, service or product. As can be seen from figure 2.7, there are many measures for usability, but the most relevant measures regarding user experience are "continuous excitement", "why and when the user experiences frustration" and "the impact of expected UX to purchase decisions'' (Bevan, 2009a). The two measures we found to be of most relevance to our topic of user experience of 2FA are marked with a blue square in the figure. We seek to know if continuous excitement is achieved by 2FA-users and potentially why and when the users experience frustration.



Measurement category	Measurement type	Measure	Area measured
Anticipation			
Pre-purchase	Anticipated use	The impact of expected UX to purchase decisions	UX lifecycle
Overall usability			
First use	Effectiveness	Success of taking the product into use	UX lifecycle
Product upgrade	Effectiveness	Success in transferring content from old device to the new device	UX lifecycle
Expectations vs. reality	Satisfaction	Has the device met your expectations?	Retention
Long term experience	Satisfaction	Are you satisfied with the product quality (after 3 months of use)	Retention
Hedonic			
Engagement	Pleasure	Continuous excitement	Retention
UX Obstacles	Frustration	Why and when the user experiences frustration?	Breakdowns
Detailed usability			
Use of device functions	How used	What functions are used, how often, why, how, when, where?	Use of functions
Malfunction	Technical problems	Amount of "reboots" and severe technical problems experienced.	Breakdowns
Usability problems	Usability problems	Top 10 usability problems experienced by the customers.	Breakdowns
Effect of localization	Satisfaction with localisation	How do users perceive content in their local language?	Localization
Latencies	Satisfaction with device performance	Perceived latencies in key tasks.	Device performance
Performance	Satisfaction with device performance	Perceived UX on device performance	Device performance
Perceived complexity	Satisfaction with task complexity	Actual and perceived complexity of task accomplishments.	Device performance
User differences			
Previous devices	Previous user experience	Which device you had previously?	Retention
Differences in user groups	User differences	How different user groups access features?	Use of functions
Reliability of product planning	User differences	Comparison of target users vs. actual buyers?	Use of functions
Support			
Customer experience in "touchpoints"	Satisfaction with support	How does customer think & feel about the interaction in the touch points?	Customer care
Accuracy of support information	Consequences of poor support	Does inaccurate support information result in product returns? How?	Customer care
Innovation feedback	User wish list	New user ideas & innovations triggered by new experiences	New technologies
Impact of use			
Change in user behaviour	How the device affects user behaviour	How are usage patterns changing when new technologies are introduced	New technologies

Figure 2.7 Categorization of usability measures (Bevan, 2009).

In the case of security systems (like 2FA) it is essential that the system is highly usable, because if not, people cannot or simply will not use it (Acemyan et al., 2018; Golla et al., 2021). According to research, users often prioritize UX over security, which demonstrates how critical UX aspects of a security system actually are (Bonneau & Preibusch, 2010; A. Das et al., 2014). Yee (2004) makes it clear that effective use and successful adoption of a security system requires careful attention to the trade-offs between security and UX. The system should adequately and specifically address trade-offs between security and UX. If this is not done, the users may find their own solutions to balance security and UX (Dourish et al., 2004).

Users can make critical mistakes when UX is neglected and that is exposing them to a greater risk than if they had a less secure system with better UX (Whitten & Tygar, 1999). Whitten and Tyger (1999) also argue that systems that have the intention of being secure, often do so at the expense of quality in UX and usability. A study done by Weir et al. (2010) found that perceived usability did not impact how willing the user was to use a given authentication technology, but rather how familiar the user was with the technology.

2.4.2 User Experience of Two-Factor Authentication

Despite 2FA's popularity and its enhancement of technological security on login solutions, multiple issues from a user's perspective are documented in research (Acemyan et al., 2018; Gunson et al., 2011a; Marky et al., 2022; Stanislav, 2015). The issues described centers around both human factors, technical matters and practical issues. A few negative experiences that are less common are also described.

Firstly, shortcomings in human aspects significantly impact the user experience. This is supported by De Cristofaro et al. (2014) who conducted a survey of 2FA users, studying the fundamental user demographics. The authors first conducted interviews with nine participants regarding popular 2FA technologies and the contexts and motivations in which they are used. The authors continued with a quantitative study involving 219 Mechanical Turk (Amazon crowdsourcing marketplace) users that aimed to measure the usability of a few 2FA solutions. They found that user characteristics, such as age, gender or education, correlate with the perception of 2FA usability, rather than which two-factor technology is used. Gunson et al. (2011a) found similar differences, i.e. that older users found 2FA less usable than younger users. Additionally, older users perceived the difference in security between the two authentication methods studied as being much less than younger users, possibly due to a lack of technical competencies (Gunson et al., 2011a). Regarding users' awareness, S. Das et al. (2018) argue that there are overall misconceptions or lack of knowledge about the security benefits of 2FA. If these benefits are not evident for the user, the users will lack motivation to adopt the second factor. The benefits of 2FA are often experienced by users merely as a cost, and not as an asset they possess, decreasing the perceived value and long-term use (S. Das et al., 2018).

Secondly, more technical issues include unsatisfactory usability in the setup process of specific 2FA tokens, lack of integration with different operating systems and low usability of the authentication process itself (Marky et al., 2022). Several other studies indicate that the setup process of a given 2FA mechanism is often perceived as less usable than the daily use (Acemyan et al., 2018; Ciolino et al., 2019; Reese et al., 2019; Reynolds et al., 2018). Further, Acemyan et al. (2018) argue that a difficult setup process can discourage users from continuing the use of 2FA.

Lastly, the user experience depends on the practical aspects of using 2FA. It requires time and effort, and users can therefore find it challenging to afford the authentication process as a part of their everyday work, especially when they are required to do it multiple times (Marky et al., 2022).

Abbott and Patil (2020) support the frequency argument with findings from a survey conducted at a large U.S. university with 40 000 students and 10 000 employees. The researchers examined years of authentication event logs at the university. The university had a multi-phase rollout of 2FA, where each phase had a different mode of authentication. During each phase, the students and employees conducted an online survey corresponding to the rollout phases. The authors found that the UX and acceptance of 2FA degraded when users were forced to use 2FA for logging into every single university resource, even if that resource did not contain any sensitive information. Users found 2FA acceptable when the requirement was limited to only a few of the sensitive systems, even if the user experience of 2FA compared to password-only authentication was unfavorable.

A similar conclusion is drawn by De Cristofaro et al. (2014), which suggests that the frequency at which users are required to provide the second authentication factor is essential to how usable they might perceive 2FA technologies. The authors give examples of institutions and service providers that request a second factor only if the user tries to authenticate themselves from an unrecognized device, such as if the cookies are cleared or from a new location. The generally low frequency might be the reason why many users perceive 2FA as usable (De Cristofaro et al., 2014). In some cases, users may not have a choice whether to use 2FA. The adoption rates will then likely depend on the user experience of 2FA.

Another consideration is the comparative experiences of the various authentication solutions and methods. An interesting observation by Gunson et al. (2011a) suggests that users tend to negatively correlate the security of 2FA with the user experience of authentication, meaning that high perceived security ratings were coupled with lower usability ratings. This illustrates the difficulty in providing usable security in a user interface. The authors investigated user perceptions of SFA and 2FA methods in automated telephone banking. Over 75% of the participants rated 2FA as the most secure, while single-factor authentication was ranked greatest for convenience and ease of use. Dutson (2019) concluded from the survey on user perceptions from Gunson et al. (2011a) that most participants have an overall preference for single-factor authentication, because people value convenience and ease of use over the security aspect.

With respect to the different methods for authentication, Abbot and Patil (2020) found that smartphone push notifications were the most widely used and preferred method for 2FA, as users found it least frustrating. Text messages, physical hardware tokens and automated phone calls were number two, three, and four, respectively.

Other studies have indicated the usability of 2FA mechanisms in various cases (Marky et al., 2022). For instance, in a study by De Cristofaro et al. (2014), the participants found one-time passwords (OTP) - delivered through text messages, -generators and apps, as highly usable. De Cristofaro et al.'s (2014) results indicate that usability, together with trustworthiness and the required cognitive effort, are critical factors in the user adoption of 2FA mechanisms. The authors in this study found that 2FA technologies are perceived as highly usable with little difference among them.

Colnago et al. (2018) also conducted a study at a university, studying the behavior and opinions of users when 2FA was made mandatory for students and staff. The initial survey was distributed prior to the mandatory adoption of 2FA and generated 1251 responses. The subsequent survey was distributed three months after 2FA was made mandatory and generated 796 responses. The findings indicated positive perceptions of 2FA and users did not find it difficult to use, however, they still found it annoying. The differences of perceptions of 2FA between early voluntary adopters and those required to adopt due to the mandatory switch, were less significant than expected. This study only consisted of surveys, while we are conducting in-depth interviews that uncover the users' whole experience of 2FA in more detail, not only perception and usability. We will in addition conduct a survey, but the informants will be employees working with technology. This could yield different results, as those employees may have different experiences than students and staff at a university.

From the theory we find that there is extensive research on both information security, including 2FA and UX. Usable security has become a recognized interdisciplinary field that aims to understand the interplay between these concepts, i.e. between human factors and security. By comparing the findings and principles from usable security to information systems and to security mechanisms, the aim is to evaluate and develop the technical solutions to better serve their purpose in a human and organizational setting. The existing literature on how this dynamic unfolds for users of 2FA in digital collaboration tools reveals that there is room for improvement in several aspects. Namely, the UX is impacted by the users' demographic, knowledge and perception of cybersecurity, the usability and practicality of the system and technical obstacles. Users also report varying experiences of the different 2FA solutions and these three factors, with their respective methods.

Our thesis will add to this body of knowledge by researching the specific case of two-factor authentication in an IT consultancy firm, and discussing how these findings can be generalized and contribute to creating more positive user experiences and enhanced security mechanisms in the future. In our research we will try to uncover employees' perception of the security benefits of 2FA and how this impacts motivations for use. Also, we want to investigate if 2FA requires too much effort in everyday work, such as a high frequency or untimely authentication requests, and if users therefore find 2FA annoying. Furthermore, we want to investigate which 2FA methods employees prefer and if this is of importance to the user adoption of 2FA.

3 Method

3.1 Introduction

When conducting empirical research, there are multiple decisions and considerations that need to be made to ensure quality in the research and results. As researchers, we needed to formulate a research question based on existing theory, choose a research design, as well as selecting a suitable method for data collection and data analysis (Oates et al., 2022). Busch (2016) argues that each level of the research method influences the next, and from figure 3.1 one can see how all the levels are connected. It is for example not recommended to conduct the data collection before the research design is finished. The different phases in the method refer not only to a practical approach to the research, but also to a systematic way of asking critical questions about the choices made and their consequences (Jacobsen, 2005). In this chapter we aim to do exactly that.

In regard to the goal of conducting empirical research, Jacobsen (2005) explains that research is not necessarily discovering some completely new knowledge or something ground-breaking, the goal can also be to develop and refine existing knowledge. This type of knowledge does not represent a break with previous assumptions, but rather an extension and supplement to what is already known (Jacobsen, 2005; Oates et al., 2022). The empirical research presented in this thesis falls into this category. There is already an extensive body of research on the user experience of 2FA, and broader topics like usable security, but our research question adds valuable data by researching user experience of 2FA within a specific context.

Jacobsen (2005) also describes how one can distinguish between three main types of purposes for the research; descriptive, explanatory and prediction. Descriptive strives to gain insight into a phenomenon. Explanatory wishes to say something about cause and effect, to explain why a phenomenon occurred. Prediction has the objective of predicting what will happen in the future. In the natural sciences, the goal of a good theory is often the ability to make predictions, while in the social sciences one is more careful with such predictive statements (Jacobsen, 2005). Our research has both a descriptive and an explanatory purpose, i.e. we want to describe the characteristics of a specific phenomenon, and why this is occurring.

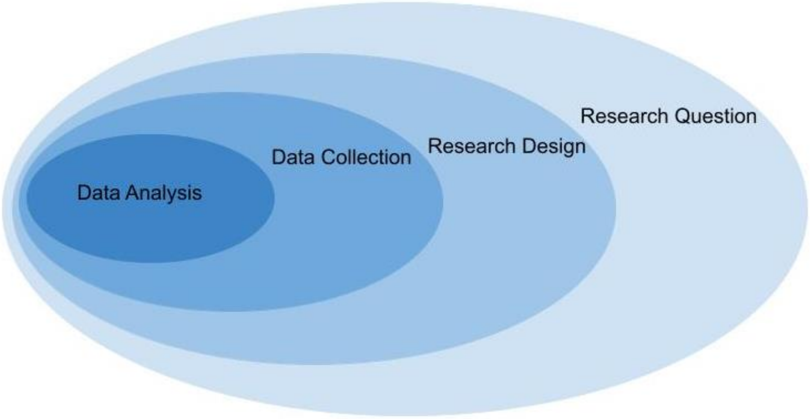


Figure 3.1 The different levels in a research method (Busch, 2016).

In figure 3.2 one can see a model of the research process for writing the thesis. This figure shows a rough overview of the progression from the start (red box) with planning, to the finish (green box) with proofreading and finalization.

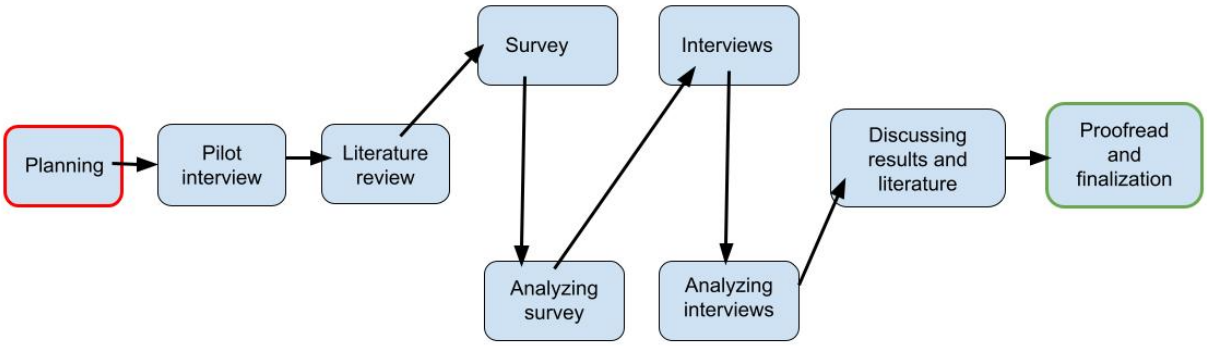


Figure 3.2 Our progression of the master thesis from start to finish.

3.2 Case

3.2.1 Case Description

Atea is a prominent IT company with a presence in the Nordic and Baltic countries. In Norway, the company boasts around 1750 employees located across various regions of the country. Of these employees, approximately 1000 work as consultants. The Norwegian division of Atea is divided into regions, with Region Nord comprising 350 employees, and Trondheim serving as its main office. Region Nord's large clients include Helse Midtnorge and Trondheim Municipality. Atea contribute to value creation for their customers through a holistic offer of products and services to the value chain.

Atea's business strategy centers around meeting customer requirements and generating value through its three core business areas, namely Digital Workplace, Hybrid Platforms, and Information Management. A central component of the Digital Workplace is the implementation of digital collaboration tools that facilitate efficient and productive communication, mobility, and work tools in organizations. These tools also ensure secure access to all applications, regardless of the user's location.

Following a discussion with Atea, we mutually agreed to focus our thesis on the user experience of 2FA in M365. This topic was identified as a potential issue within their organization. To undertake this research, we collaborated with Atea's End-User Computing team, based in Trondheim, which specializes in M365 and user-related technology adoption and optimization processes. This team is responsible for integrating physical devices, software, and solutions to create the most optimal user-technology experience.

3.2.2 Microsoft 365

Atea utilizes Microsoft 365 as an internal tool and also offers it as a complete service to its customers. The company provides guidance and support to customers throughout the implementation process, from identifying potential opportunities to planning and executing the technical solution, in addition to user adoption. Atea also offers continuous user support and optimization, as well as further development of the tool within the company. The company's comprehensive approach ensures that customers can successfully implement and maximize the benefits of Microsoft 365.

Upon employment, Atea employees are automatically assigned a Microsoft Enterprise 5 license (Microsoft E5), which includes the entire portfolio of Microsoft 365 applications. Although all applications are available within the portfolio, not all may be in use by a particular organization. Microsoft offers three enterprise plans, as depicted in figure 3.3. E5 is similar to Enterprise 3 (E3), but with additional security features, such as threat protection, information protection, and advanced compliance. The threat protection feature enables the detection and investigation of advanced threats, while information protection secures sensitive data throughout the organization. The advanced compliance feature allows companies to assess their compliance risk using simplified assessment tools. Additionally, E5 includes Power BI Pro, an advanced analytical tool that helps employees work smarter and make informed decisions quickly. Power BI Pro is represented by the black symbol on the right of figure 3.3, under "Office Applications," and is only available in E5.

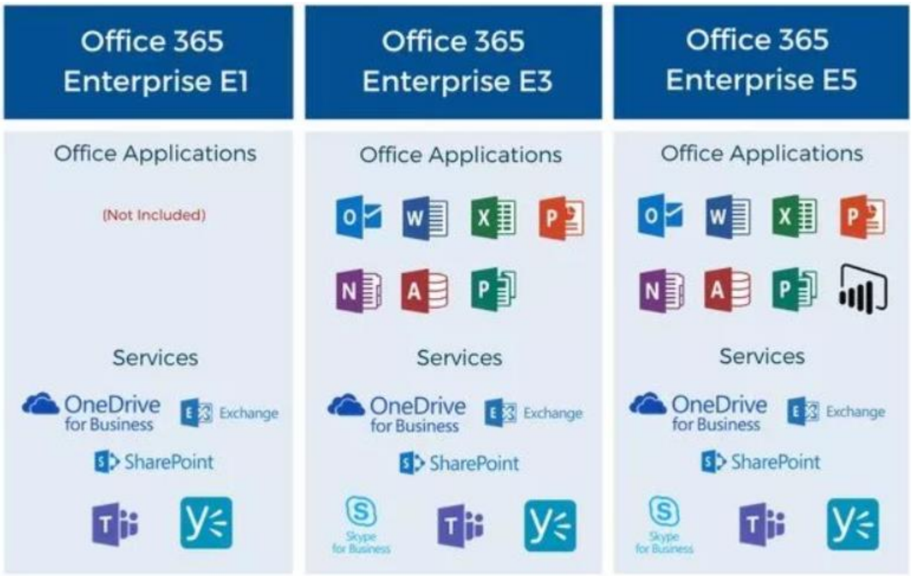
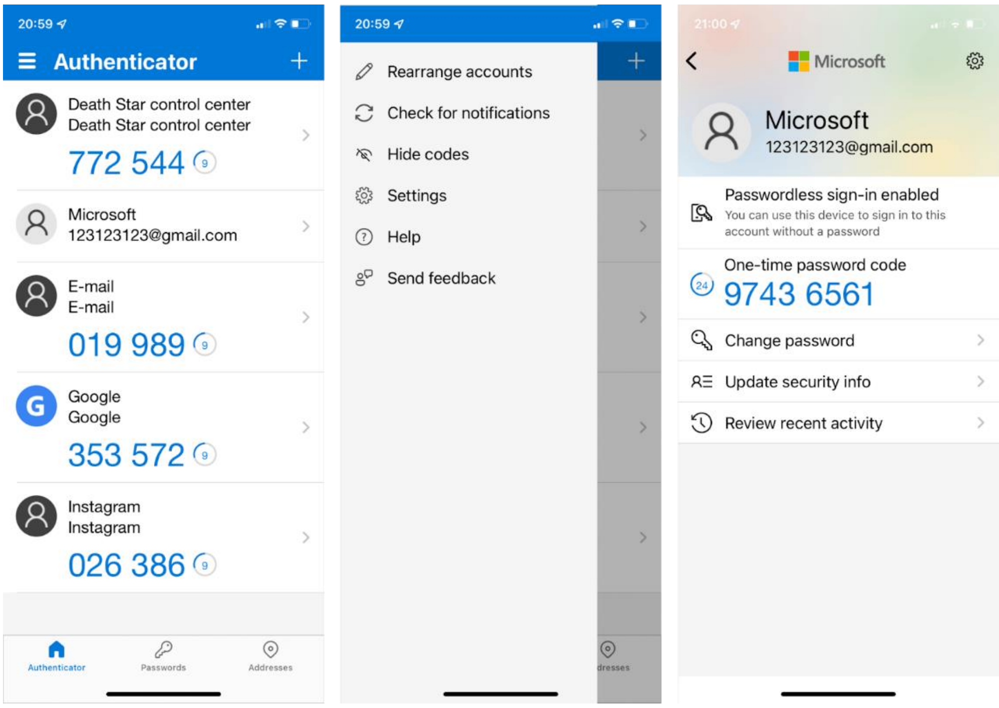


Figure 3.3 The different enterprise plans from Microsoft 365.

3.2.2.1 Microsoft Authenticator App

The Microsoft Authenticator App is the recommended 2FA app for Atea employees to securely access systems like M365. It is considered the most secure solution for 2FA from Microsoft and the design can be seen in figure 3.4. When logging into Microsoft, employees receive a prompt in the app that they need to approve. Additionally, the app offers one-time passwords as an alternative solution. Throughout our thesis, we also refer to the Microsoft

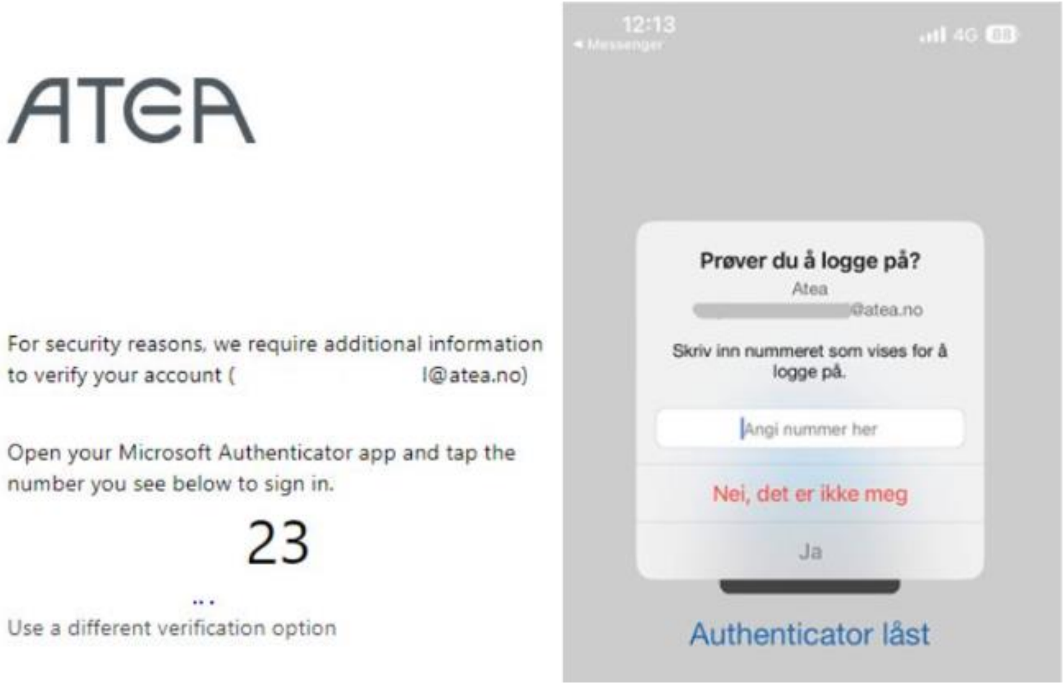
Authenticator App as "the app" since it plays an essential role in our research question concerning the user experience of 2FA in Microsoft.



You can use this device to sign in to this account without a password

Figure 3.4 Microsoft Authenticator App.

In October 2022, Microsoft announced that a number matching security feature would become default for all organizations using the Microsoft Authenticator App. Originally scheduled to be enforced starting February 27th, 2023, the rollout was extended to May 8th, 2023, following feedback from customers. This new feature requires employees to enter a number in the app to authenticate, serving as a safeguard against accidental approvals and MFA fatigue attacks, where attackers spam target victims with MFA push notifications (Gatlan, 2023). An example of an authentication request with the number matching feature is shown in figure 3.5. This upgrade requires Atea and its customers to update their MFA routines. On February 20th, 2023, a statement was issued to all Atea employees notifying them that starting from February 23rd, they would need to complete the number matching process when using the app to authenticate (see figure 3.6). Additionally, users will receive the name of the application that requires the authentication.



ATEA

For security reasons, we require additional information to verify your account (l@atea.no)

Open your Microsoft Authenticator app and tap the number you see below to sign in.

23

Use a different verification option

12:13
◂ Messenger
4G 88

Prøver du å logge på?

Atea

[redacted]@atea.no

Skriv inn nummeret som vises for å logge på.

Angi nummer her

Nei, det er ikke meg

Ja

Authenticator låst

Figure 3.5 The number matching feature in Microsoft 365.

In addition to the Microsoft Authenticator App, Atea provides its employees with the option to receive a unique numeric code via SMS or phone call as part of their 2FA process. After entering their password, employees receive the code which must be typed in to complete the login process. A phone call option is also available, where the code is read out loud to the employee. Furthermore, for certain internal systems, Atea uses the Entrust app as an authenticator, which provides even greater security than Microsoft. This is specifically used for particular applications or when accessing the virtual private network (VPN) from outside of the office. Further, a large majority of Atea employees use computers that are configured with a standard Atea image. This configuration is designed to minimize the number of times employees are prompted to authenticate themselves throughout the workday.

3.2.3 Training for Employees

Atea offers two types of training to its employees. The first is workplace behavior training, which covers a wide range of topics, including information and non-disclosure agreements, which are critical for maintaining information security. Atea employees have access to sensitive customer information and must behave responsibly. The behavior training also includes other essential topics, such as employment procedures and the code of conduct, which is a mandatory document that outlines guidelines for issues such as money laundering and accepting gifts from customers.

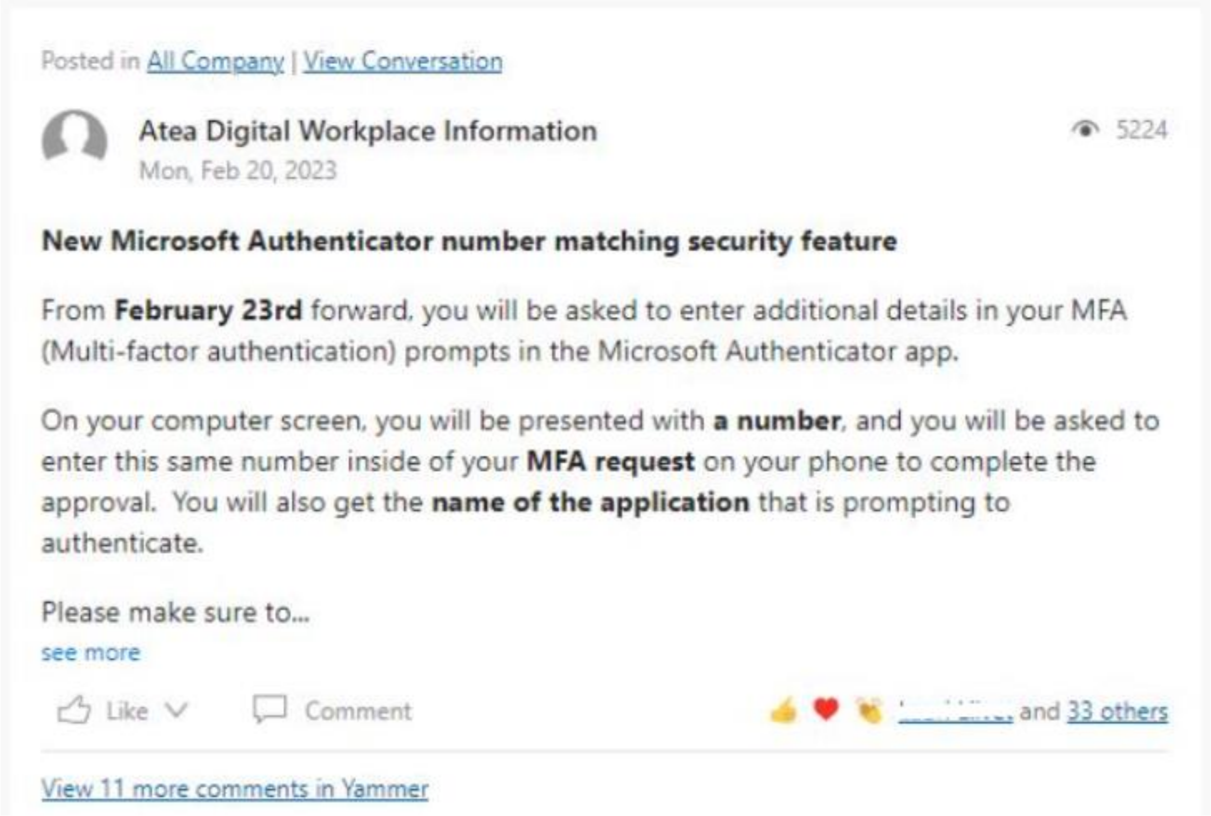
Atea provides a gamified e-learning system called Motimate as the second type of training. This system aims to create an enjoyable experience similar to playing a game, with the goal of motivating and exciting employees to complete courses. Motimate offers different courses customized for leaders and employees in various areas, including security. While the system is not mandatory to complete, it contains valuable information that employees are encouraged to read. Therefore, employees often use Motimate as a "just-in-time" resource when they encounter a problem. The courses in Motimate are also designed to provide critical information, such as security-related topics, and to enhance the knowledge and skills of the employees.

Atea provides internal webinars to educate its employees on the practical usage of digital collaboration tools. These webinars cover e.g. the correct usage of tools such as Teams and the optimal way to structure OneNote. While most new hires have prior experience with M365, they can still attend these webinars or complete relevant courses in Motimate for additional training in their competencies. The primary objective of these webinars and courses is to raise awareness and train users on the appropriate use of these tools. Some employees have faced challenges when their colleagues use tools incorrectly without proper training, which is why these webinars are crucial for effective tool usage.

As an IT consultancy firm, Atea has expertise in IT security and provides several operational security services to their customers. One such service is Atea's Security Operations Center Plus (SOC+), which monitors IT systems and networks for security-related incidents. Its purpose is to detect and prevent malicious activity, as well as investigate suspicious behavior. In the event of an unwanted occurrence in their IT environments, Atea's Incident Response Team (IRT) is available to respond. As more companies prioritize cybersecurity, authentication vulnerabilities should be reduced, leading to fewer security incidents. However, cyber attacks against businesses are continually increasing. Therefore, it is crucial for Atea to ensure that their IT security experts are highly skilled and up to date in their professional field. It is important to note that their training is tailored to the specific services and products they offer to their customers and not for internal scenarios as casual users of digital tools.

3.2.3.1 Training in Two-Factor Authentication

Employees of Atea get no formal training in the Microsoft Authenticator App. Nor in the Entrust authentication app do the users in Atea receive training. Atea provides minimal training to employees on 2FA. Occasionally, the IT department would send out an email informing users of any changes to the authentication process, such as alternative login procedures or instructions on how to handle specific situations. However, this training is limited in scope and does not provide detailed guidance on best practices or potential vulnerabilities. An example of this can be seen from figure 3.6, when number matching was implemented. The announcement was posted in the company-wide group on Yammer (M365’s enterprise social networking service), with some quick instructions. Still, this is just an informational post or email, not training through practice over time.



Posted in All Company | View Conversation

Atea Digital Workplace Information

Mon, Feb 20, 2023

5224

New Microsoft Authenticator number matching security feature

From **February 23rd** forward, you will be asked to enter additional details in your MFA (Multi-factor authentication) prompts in the Microsoft Authenticator app.

On your computer screen, you will be presented with **a number**, and you will be asked to enter this same number inside of your **MFA request** on your phone to complete the approval. You will also get the **name of the application** that is prompting to authenticate.

Please make sure to...

see more

[redacted] and 33 others

View 11 more comments in Yammer

Figure 3.6 The announcement made to the employees on Yammer, stating that a new number matching feature was implemented in Microsoft 365.

It is natural to assume that people understand *how* to use the authentication app, as it is remarked that it is used by almost all employees several times a day. However, it is uncertain to what extent the users understand *why* they have to authenticate, and why it is important. For instance, there have been instances where employees prefer to save an online document in a location that does not necessitate 2FA rather than saving it in a secure and compliant storage location that requires 2FA.

Some of Atea's customers have been encouraged to turn on 2FA for the first time, but most companies have already implemented this as a security mechanism today. Atea has helped customers experiencing significant security breaches as a result of only utilizing usernames and passwords (i.e. single-factor authentication). Non-technology related organizations often use information technology as a supportive tool for certain business functions out of necessity, and do not regard information technology at the core of all business operations. These types of companies are usually less concerned about information security, including the importance of 2FA, and thus even less concerned with training and educating their employees. It is important to note that when Atea consults businesses, they are usually never responsible for training the employees at the customer company. They occasionally give some guidance, but they generally only manage and execute more technical issues such as operations, security and maintenance, as well as project management and advisory. Hence, this responsibility lies on the customer and they have to determine what training they wish to pursue and to what degree it should be undertaken.

3.3 Research Design

3.3.1 Research Question

When deciding upon the most appropriate research design, the research question is at the core (Oates et al., 2022). The research question not only states what is being studied, but equally important how the research is delimited, i.e. what is *not* being studied.

The formulation of our main research question indicates that it is both a descriptive and an explanatory type of research question. We aim to describe the current user experience of a given technology (i.e. two-factor authentication in M365), limited by time and space. We also try to explain the causality between some phenomena. We do however not attempt to test a hypothesis. The creation of the research question was an iterative process where the exact formulation came along as we became familiar with theory and empiricism.

3.3.2 Extensive or Intensive

Extensive and intensive describe two fundamental designs for research, Jacobsen (2005) explains. Extensive research is best suited for a confirmatory research question. The purpose of a confirmatory research question is to map the scope of a phenomenon, and thus extensive research pursues breadth and quantity. Consequently, quantitative methods are best fitting for extensive research design. In contrast, intensive research seeks to explore nuances and depth, and is therefore more sensitive to contradictions and contextual conditions. Intensive research is therefore used to answer exploratory research questions, as it is more focused on fewer examined units. Consequently, qualitative methods are best fitting for intensive research.

The nature of our research question combined with the specific case makes it arguably both extensive and intensive. UX is a multidimensional and dynamic phenomenon, it is highly personal and at the same time highly contextual, shaped by constantly evolving internal and external factors. We are researching the collectiveness of the UX - as it exists and unfolds within a larger group of M365 users. Extensive research will be fitting to explore the broader trends among the researched phenomenon within our case, and the extent of these trends across individual users. Intensive research will be necessary to thoroughly understand and analyze the individual user experiences of our participants.

The extensive research, in the form of a questionnaire, was conducted first. This way we could confirm the findings from the literature and concurrently get input to narrow down and specify our questions to the in-depth interviews, and to an even greater extent make the interviews intensive.

3.3.3 Quantitative or Qualitative

Quantitative and qualitative methods are the two main paradigms to gather knowledge about the society and to make analyzes (Oates et al., 2022; Tjora, 2019). Busch (2016) states that the method chosen is closely connected to the research design.

When conducting quantitative methods, one usually operates with numbers and sizes, and the goal is collecting data from a broad sample. Quantitative surveys do not provide insights into *what* and *why*, but provide the answers to *how much*, including the positive and the negative, regarding the research question (Berg & Lune, 2017). When collecting data, Jacobsen (2005) points out how it is a prerequisite for the researchers to have an adequate overview of the variables and the phenomenon that the research question aims to answer. The researchers will then be able to meaningfully define the phenomenon and make predefined answer options that facilitate the respondents to effortlessly contribute with their experiences and opinions.

Qualitative methods aim to focus deeply on personal interpretations and reflections (Jacobsen, 2005). Usually, one focuses on a small sample to gather real-world information concerning a problem, especially where phenomena are unknown, or where one has the need for additional information (Johannessen et al., 2011). Tjora (2019) states that these types of examinations normally concentrate on obtaining knowledge, rather than obtaining explanations. This is useful in situations where the research question is complex, and the researchers have to show empathy and creativity to discover the answers. Quantitative methods are therefore most preferable with extensive design that pursues breadth and quantity, while qualitative methods are most preferable when the design is intensive; i.e. few respondents and numerous variables to analyze (Jacobsen, 2005).

	Quantitative Data	**Qualitative Data**
Should be used when we have	Good knowledge and understanding of the phenomenon we are going to study	Poor knowledge of the phenomenon we are going to study
When we shall	Test theories and hypothesis	Develop new theories and hypothesis
When we have	A wish to generalize (know a little bit about many)	A wish to have a great deal of information about few entities
When we will	Find out how often a phenomenon occurs	Find out what the phenomenon contains
Advantages	-Many entities -The possibility to generalize from the selection to the population with a high degree of certainty -Relatively low costs	-Depth and understanding of details -Holistically understanding of a phenomenon -Flexibility in the data collection
Disadvantages	-Superficial information -Rigidity in the data collection -We force people to special meanings through standardized questions and multiple-choice options. -Analytical distance can give a low understanding	-Unclear and too detailed information -Too much flexibility can result in the research never being done -High costs, especially in the analyze phase -Proximity to the participant can destroy the ability to analytical distance

Table 3.1 Overview of the differences between the research methods (Jacobsen, 2015).

As can be seen from table 3.1, the two methods have some advantages and disadvantages. The table also shows in which situations each of the methods are most suited, based on what we wish to do and what we aim to find out. We wished to combine the methods so that they complement each other. First, we used a quantitative method to test our assumptions on a large group of employees, and then we used a qualitative method to obtain a deeper insight about the phenomenon.

Because we aimed to discover how the users experience 2FA, we needed to have a conversation with the users, i.e. the interviewees. We needed to be able to ask follow-up questions and uncover all their true feelings concerning the topic. We decided to do a survey on employees of Atea Region Nord as the first data collection. This would give us an overview of how many employees have experiences of 2FA solutions from M365. We used these answers to shape the interview guide. The interviews have been our primary method of collecting data, as the interviewees could share their experience in more detail. We also had the opportunity in the interviews of asking questions regarding some general answers from the survey.

3.3.4 Time Limit

An important question to consider was whether the data should be collected during one or more time periods. Johannessen et al. (2011) distinguishes between longitudinal studies and cross-sectional studies. Longitudinal studies research the same people over the course of several time periods. This is the ideal because the data collection at repeated times can make it possible to analyze complex developmental features and study the cause-effect relationship (Busch, 2016). A cross-sectional study is the other option, which gathers data at one point in time. Because of our limited available time and resources, we were forced to conduct a cross-sectional study. Our quantitative data collection carried on for one week, while our qualitative data collection carried on for approximately two weeks. This is still categorized as a cross-sectional study because we only distributed the survey once and only conducted one interview for each participant. As Jacobsen (2005) states, this study cannot help us to see contexts or to discover if the results could be different if the study was done at other times.

3.3.5 Design Decision

3.3.5.1 Case Study as a Method for Research

The central phenomenon we wanted to study in our research was the user experience of 2FA. We also specifically sought to understand how the specific context - in M365 provided by an IT company - facilitates and shapes the experience. It is this limitation in time and space that makes this a case study (Jacobsen, 2005; Oates et al., 2022). Specifically, a popular definition from Yin (2009) states that a case study is "an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (p. 18). In other words; case studies are highly applicable to contemporary situations of real, human life and interdisciplinary areas (Oates et al., 2022; Quintão et al., 2020). Our research question covers these properties, as it combines both a technical solution and the very human experience, all set in a specified real-life, contemporary situation. Specifically, the case of this thesis is a type of collective case, because it involves studying multiple single unit cases simultaneously (single unit cases being each individual M365 user) (Jacobsen, 2005). All this implies a level of complexity in relationships and processes that the research design must be able to capture.

3.4 Method for Collecting Data

3.4.1 Survey

Before finishing the redesigning of the pilot interviews, we chose to conduct an online survey to gather information from numerous users. This decision was made because we wanted the perspective of the user experience of 2FA from a multitude of users. The survey made it possible to gather data on a large scale, and made it less complicated for us to discover which factors made the greatest impact for the users. The survey was based on theory and understanding from previous research combined with several questions from the pilot interviews. Before distributing the survey to employees at Atea, we carried out five pilot surveys. This was done mainly to get feedback and improve the questions before distribution.

We aspired to get as many experiences, opinions and point of views about the phenomenon as possible. Since the number of interviewees is smaller than the number of participants that conducted the survey, the interviewees would only give us a limited number of experiences and opinions. For this reason, we used the answers from the survey as part of designing the interview guide, because it could help us to see which experiences, opinions and feelings were most common, and could be discovered in more detail in the interviews. With conducting a survey we were able to gather a considerable amount of data within a short timeframe, which is a significant advantage with surveys, according to Jacobsen (2005).

The survey was made through Nettskjema, which NTNU has a data processing agreement with. Nettskjema is a secure solution made by the University of Oslo. Nettskjema is the most used and most secure data collection tool in Norway (*Nettskjema*, n.d.). The solution is flexible and can be used for both large data collections and surveys, and can be conducted on both the computer and the phone. The questionnaires are encrypted and kept in secure storage in Service for Sensitive Data (TSD) (Gulbrandsen, 2017).

We conducted the survey prior to the new change from Microsoft regarding the Microsoft Authenticator App, notified at Atea on February 20th, 2023 (stated in section 3.2.2.1). At the time of the survey, the employees did not use number matching when approving authentication requests in the app, nor did they get the name of the application that prompted to authenticate.

3.4.1.1 The Structure of the Survey

The survey was in the form of a questionnaire, with single-answer or multi-answer options. We also had one question in the form of a range. The purpose was to gather plentiful information. The survey consisted of four different sections, each covering separate areas. The respondents had a progress bar at the top of the page during the entirety of the survey, motivating them to finish. The first section consisted of background questions, like their age, gender, if they work with security or not, if they use the Microsoft Authenticator App etc. Section two consisted of a matrix with different statements regarding the Microsoft Authenticator App, and options ranging from "strongly disagree" to "strongly agree". This section was not visible to respondents that previously answered that they never use the app. Section three consisted of a similar matrix, but with statements concerning security breaches, training and security culture. The last section had questions with single answer and multi-answer options regarding two-factor authentication, possible challenges and motivation for use.

Fixed questions with multiple-choice answers implies a standardization where it is facile to compare similarities and variations in the way the respondents have answered. The degree of standardization in surveys compared to in-depth interviews provides greater possibilities for generalization from sample to population (Johannessen et al., 2011; Oates et al., 2022). There exist a number of drawbacks that were taken into consideration during the survey process. Firstly, the possibility of crucial information being omitted due to the inability to pose follow-up questions or clarify questions that were not understood by the respondents. Secondly, the respondents could feel compelled to provide answers to questions that they were unsure of. To mitigate these issues, the survey questions always contained answer options for "I don't know/not relevant" and "Other:...", enabling respondents to express their thoughts or provide their own answers when the given options did not align with their opinions. This approach ensured that respondents could always add their own response if they felt none of the options were correct and that no respondents answered a question without knowing what the question entailed.

The questions in the survey were formulated to best shed light on the research question, as specific as possible. We also tried formulating the questions so that all respondents interpreted them in the same manner, despite the selection having very diverse backgrounds and knowledge regarding the topic.

3.4.1.2 Recruitment and Selection

Our contact person suggested distributing the survey to all employees of Region Nord, because our current location is part of this region. We decided to limit our survey respondents to this region. This could potentially give us 350 answers, but we were able to receive 122 answers. Jacobsen (2005) states that dropouts are fairly common in surveys and that this might be one of the most substantial disadvantages with surveys. In an effort to increase participation, we introduced the survey during the first presentation we had at Atea, but it was unfortunately only attended by 15 employees. Our contact person at Atea provided information about the survey and the link to the survey via email to all the employees of Region Nord. To get a satisfactory overview of how the users in general experience 2FA, the respondents had to be employees with different positions and competencies.

3.4.1.3 Distribution and Implementation

The respondents received a link to the survey at their company email. To get access to the survey, they needed the link from the email, which was distributed only to employees of Region Nord of Atea. The survey was available on the internet for one week. Two days prior to the deadline of answering the survey, our contact person sent another email reminding employees to participate.

Of the 122 respondents, almost 51% were consultants, 4,1% worked in administration, and the rest was distributed evenly between Atea Managed Services, sales and solution sales. Over half of the respondents work with security. We are satisfied with the amount of respondents.

3.4.2 Interviews

The preparations for the interviews for this thesis started already when conducting the pilot interviews. Conducting the pilot interviews was very beneficial for us for many reasons. It gave us some valuable experience of the role as interviewers, the opportunity to test out the quality of the interview guide including the questions, and it gave us feedback that helped shape and develop the research question. We conducted two pilot interviews with two different employees at Atea. Both employees had long and broad experience with M365, and were both experts in the End-User Computing team, in addition to being regular users. The main findings from the interviews were supported by findings in the literature; namely how 2FA is part of the workday in a practical sense, how it is experienced by users and how this is part of a greater security culture. The interview guide changed slightly after the pilot interviews, to better fit casual users.

Interviewing is the most widespread method of collecting data as qualitative research (Tjora, 2019), and we chose to conduct in-depth interviews. The goal of the interview is making the participants reflect upon their experiences in relation to our topic of 2FA. We used open questions so the participants could provide as long answers as they saw fit. They would also have the opportunity to talk outside the questions, making digressions in a way that could be relevant to our topic. If the participants did not understand the questions or if the circumstances needed to be explained, this could be done through the in-depth interview.

In-depth interviews, also called semi-structured interviews, are suitable when we want to explore (rather than check) personal accounts and feelings (Oates et al., 2022), and therefore chosen for our study of opinions, attitudes and experiences of 2FA in M365. It might be possible to study this in another way, but talking to employees and really listening to their experiences and meanings are beneficial with interviews. Sometimes when conducting interviews one might get information and different perspectives that were not a part of the plan (Oates et al., 2022). This opportunity for the participants to open up will generate more data for us to analyze, but could give important insights for our research.

The research question in this thesis is complex, which makes it necessary for us to analyze the interviews and compare them to each other, and then draw conclusions. Our chances of getting the relevant information that we are seeking are higher when conducting in-depth interviews. We would map the most important experiences employees have made through using 2FA. We could also discover which training methods the participants value the most.

The interviews were recorded and transcribed using digital tools. For interviews conducted online in Teams, we used the built-in transcription function. We also recorded the interviews, to make sure we had a backup if one method failed. For interviews conducted in-person, we used the Nettskjema-Diktafon app, an app by Nettskjema for secure and encrypted sound recording. This is the only app NTNU recommends to collect and store personal data on private equipment. We simultaneously recorded the interviews using Teams on our computer, as recommended, as there have previously been reported technical instabilities when storing recordings in Nettskjema Diktafon. The recordings were then transcribed using the built-in function in the online version of Microsoft Word.

The interviews were conducted after Microsoft issued the new change to the Microsoft Authenticator app, where number matching is required when using the app (section 3.2.2.1). This change in MFA-routines at Atea were taken into consideration when conducting the interviews. Users will additionally get the name of the application that prompts authentication.

3.4.2.1 The Structure of the In-Depth Interviews

The structure of the interviews in this thesis was based primarily on Aksel Tjora's recommendations in his book "Qualitative Research as Stepwise Deductive Induction" (Tjora, 2019). The interviews should roughly be categorized into three phases: warm-up phase, reflection phase and winding-up phase, as can be seen from figure 3.7. It shows that most reflection is done halfway through the interview. Each phase contains different types of questions and the reflection from the participants will vary in depth and length. To keep a good structure, it is recommended to use an interview guide, as we chose to do. The interview guide contains questions for each of the three phases and that helped us to stay on track. The questions were based on the pilot study that we did in the previous semester, the theory we studied in the beginning of the research process and the answers to the survey we conducted.

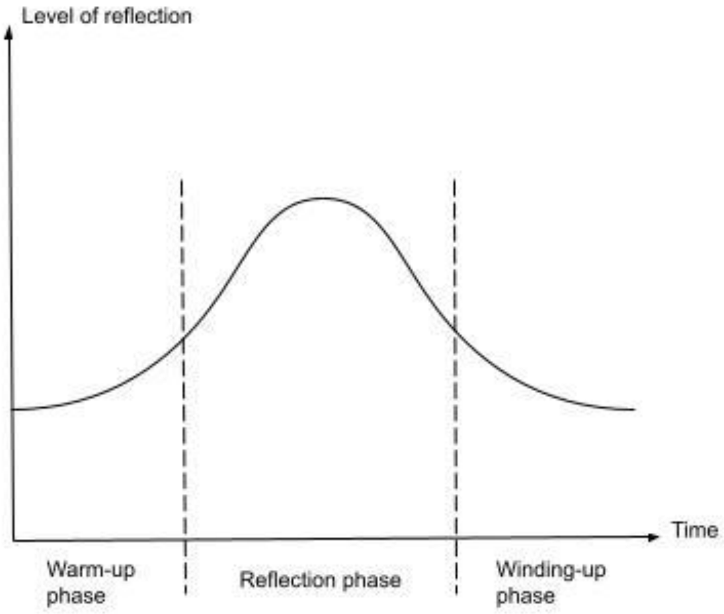


Figure 3.7 The phases of the in-depth interviews (Tjora, 2019).

The interviewees received an invitation to participate in the research project prior to the interviews (see section 3.4.2.2). We sent them a contract that presented the topic of the interviews, the purpose of the interviews, what their contribution would entail, rights, privacy and other matters. It also included how the data would be saved and treated throughout the research project. This contract was compiled and approved by Norsk Senter for Forskningsdata, NSD (see appendix A), and the participants gave their consent before the interviews (see appendix B).

The interviews started with us presenting ourselves and presenting the topic of the research project. We gave the participants information about their rights, e.g. that they could withdraw from the interview at any time without giving a reason. If the interview was conducted remotely, we asked for their consent in recording a video, otherwise we asked for consent to record an audio file. We answered all potential questions the participants had before starting the recording and the interview. The interview started in the warm-up phase with simple and specific questions regarding the role of the employee, their responsibilities, their tasks, previous experiences and projects etc. The questions were mainly used to categorize the employees based on their knowledge, because they can contribute with different insights into the project. This warm-up phase was meant to "warm-up" the participants, i.e. to make them comfortable in the next phase.

The next phase was the reflection phase, containing most of the fixed questions for all participants. These questions were the main ones in the interview that consisted of the experiences with 2FA, possible challenges with 2FA, if they believe the training in 2FA is sufficient, if there is a good security culture at work, what their motivation is to use 2FA etc. We also had a few questions specifically for employees that have implemented 2FA at a customer company. Each of the topic areas had several questions to get deep into the participants' perceptions and experiences. When necessary, we rephrased the questions or asked them follow-ups, making sure they fully understood the questions and were able to express all their feelings and opinions regarding the topic. Follow-up questions were not planned for, but done to adapt to the different answers. Some participants needed all questions from the interview guide to get a good structure and express their feelings, while others talked so much around the topics that they did only need the interview guide once in a while. The interview guide was therefore not strictly followed, but was used to ensure that all topics were visited.

As part of the winding-up phase, we gave a brief summary of the key-takeaways from the specific interview to confirm that we understood the information and to check if the participant had something to add. We took this time to also inform the participants about the next parts of the research project and how they could get access to the thesis. We thanked them for the participation and were available for further informal conversation, if desired. All the participants said to contact them if we needed supplementing information.

After completing the first three interviews we made some valuable experiences that led us to remove a question, and add another, which can be seen in the interview guide in appendix C. Firstly, we became aware that the employees did not set up the Microsoft Authenticator App themselves on their phones, nor did they remember their experience of doing so. Therefore, there was no point in asking about this. Secondly, we realized that when asked if and how they work with IT security, they would often answer in terms of a consultant perspective, how IT security is a part of their portfolio, and not as a part of their smaller, everyday work routines. Therefore, we added a question asking them how aware they are of security in their own digital work, to highlight this aspect of their relationship to IT security.

The length of the interviews varied between the participants. The shortest interview lasted for approximately 15 minutes, while the longest lasted for approximately 29 minutes.

3.4.2.2 Recruitment of Participants

The process of recruitment of participants for the in-depth interviews started with a conversation between us and our contact person at Atea. We discussed what type of people could be relevant to our research project. We agreed that the HR manager would be the first to initiate contact with potential employees for the interviews, because they know casual users to a greater extent than our contact person, and therefore helping us get a wider selection. We also thought that it was more likely for employees to participate when someone from the company made the first contact.

The recruitment process consisted of the HR manager distributing an invitation to possible participants at their company email address. This email consisted of an introduction to the research project and the NSD consent form attached with information about participation etc. We received the email addresses after employees were positive to participate and we scheduled an interview at a time convenient for them. Our contact person could then book a room for the interview if it were to be conducted physically. We contacted the employees most relevant to our current topic at hand, or if we wanted a different perspective on the same topic.

3.4.2.3 Selection of Participants

The main rule for selecting participants to in-depth interviews, is to choose participants who for any reason will be able to reflect upon the topic in question (Tjora, 2019). This is called a strategic or theoretical selection. As for case-studies, such as ours, the selection of participants will be limited by a natural unity that exists independently of the study, e.g. a company. The purpose of the study is to seek knowledge about a phenomenon that is related to the case.

The goal of the in-depth interviews was to collect information from employees that had knowledge in using 2FA in M365 in Atea. The participants were selected from the employees in Atea Region Nord with this experience. Some employees worked in End-User Computing, and the rest in other departments.

The most difficult task was to identify the employees with the right knowledge and the right experiences for the interviews. We partly used the snowball sampling method, (Tjora, 2019) which is a strategy where we started with a small sample, and then got tipped off with new potential participants. Initially, we lacked sufficient knowledge regarding the most suitable participants. However, with the aid of our contact person and the HR manager, we identified the relevant individuals, as aforementioned. Our original plan, which we were able to follow, was to interview employees with different roles; some consultants, some leaders, some experts and some everyday users. Table 3.2 shows an overview of the selection of the participants, which includes their position at the company and their area of knowledge.

The overview shows the nine employees we interviewed, interviewee A-I. They all have experience from using 2FA in M365, even though they have different positions and areas of expertise. The selection consists of three managers, four sales advisors and two consultants. The sales advisors worked with a wide variety of Atea's portfolio. The two consultants worked both specifically with digital collaboration tools.

Interview	Position	Knowledge Area/Competency
A	Regional manager for collaboration and solution sales	Sales and design of audio- and visual-solutions.
B	Account manager in sales	Sales of the entirety of Atea's portfolio, customer relations.
C	Solution advisor on support agreements	Sales, management and advisory for service- and support-solutions for data rooms.
D	Solution advisor in managed services	Advisory of as-a-service solutions, concept-development and facilitation.
E	Senior security architect in solution sales	Uncover the needs of customers and sell products and services to them.
F	Solution advisor client	Advise customers with sales within the client area, i.e. screens, computers, etc.

G	Business manager	Developing the organization and internal communication.
H	Consultant	User adoption and training with customers in digital collaboration tools.
I	Senior consultant	Planning, strategy and user adaptation of collaboration tools, mostly M365.

Table 3.2 Overview of participants from in-depth interviews.

3.4.2.4 The Location of the Interviews

As researchers collaborating with Atea, we were afforded the privilege of utilizing all of their meeting rooms. To ensure availability, we provided advanced notice to our contact person who subsequently reserved the necessary meeting room for us. We could easily conduct almost all the interviews at Atea's offices in Trondheim. As we were situated at their office buildings twice a week, we tried to arrange the interviews on these days, while maintaining the option to reschedule if necessary to accommodate the participants' schedules. There were several advantages associated with conducting the interviews at this particular location; the employees were in a safe and comfortable space, they were familiar with the meeting rooms and their location, and the interviews could be conducted efficiently and effectively during an otherwise busy workday.

We did two interviews digitally in Microsoft Teams. These employees were not located at Atea Trondheim and for practical and financial reasons it was necessary to conduct the interviews online. In-depth interviews should, regarding Tjora (2019), be conducted face-to-face between the interviewer and the participant because of body language. This is why we conducted the online interviews with both audio and video in Teams, to simulate a physical presence.

3.4.2.5 The Role of the Interviewers

There are several factors to consider as interviewers. We tried to stay professional and neutral during the interviews, as well as showing interest, respect, empathy and understanding. This is important because the quality of the interviews will depend on the trust and perception that is made between us as interviewers and the participants (Jacobsen, 2005; Oates et al., 2022). This is the reason why we tried to create a safe space for the participants, where they could trust us and be an authentic version of themself. We strived to create a good atmosphere with open and positive attitudes, meaning that we always came to the interviews with a good mood and positivity. It was important to us that we did not interrupt the participant at any time during the interview. Sometimes people made digressions, but rather than stopping them we chose to ask them questions to gradually get back to the interview guide. If something came up during the interview, we would wait until a suitable moment to bring it up.

It was also important to us that the interviewees felt that their opinions and experiences mattered, we therefore said "mhm", "yes" and "I see" to acknowledge their answers. We also spent some time rephrasing questions that some found difficult to understand, because everyone should always know what they are answering. Overall, we attempted to appear as professionals. We always came to the interviews prepared; with the interview guide as a structural plan, the computer ready for recordings etc. Since the interview was always recorded, we could focus our job on the conversation and the interaction with the participant. Jacobsen (2005) points out that this type of data is ideal when it comes to qualitative research. To create a good relation between us and the participants, we dressed in a similar way as the employees at Atea, so the participants did not think of us as strangers.

We always remembered to thank the interviewees for their valuable participation after the interview was finished. Several of the participants made informal chatting when the interview was done, which usually means that they had a pleasant experience.

3.5 Analyzing Data

The analyzing phase is at the heart of the research process, and it is crucial to succeed at this for the research to deliver value to the reader through extending their knowledge on the subject area (Tjora, 2019). Analyzing data is about deconstructing and reconstructing the generated data, while maintaining critical thinking about the data and the research questions they are supposed to answer. This way relevant and significant empirical evidence can be used to answer the initial research question (Tjora, 2019). The next paragraphs describe how the quantitative and qualitative data were analyzed, respectively.

3.5.1 Quantitative Analysis

After conducting the survey, Nettskjema had several possibilities in processing the data. In Nettskjema we could see reports containing answers to questions including visual explanations. We could also download an Excel-file with a structural overview of all respondents. We mainly interpreted the visual explanations with their belonging text and analyzed the answers where respondents wrote their own answer. The results are presented in chapter 5.

Prior to making graphs and analyzing the answers, we started by shortening the statements from both matrices from the interview guide in appendix C: one concerning the Microsoft Authenticator App and one concerning IT security. In Nettskjema, we could easily view a report containing everything each respondent answered, in addition to the amount and percentage of how many respondents answered each option for each question in the survey. The statements presented to the survey respondents were both positively and negatively worded, to minimize extreme response bias and acquiescent bias. From these matrices we could see how many respondents answered each score on a scale from "strongly disagree" to "strongly agree". These numbers were difficult to analyze, so we decided to present it in a more visual way, with the average score of each statement. We continued by plotting all the numbers into a table and calculating the average score. This calculation is explained in appendix D. Because we put the statements in a table, the statements needed to be more readable, i.e. shorter, and is the reason why we have shortened some of the statements in the figures.

The last three questions, regarding challenges, why they experience challenges and motivations for using 2FA, were all multiple answer questions, meaning that respondents could tick several boxes. Consequently, we opted to include the number of respondents who answered each question in the graphs, as opposed to expressing the data in the form of percentages, as we have done in the other questions.

3.5.1.1 Correlation Analysis of Quantitative Data

After retrieving the data from Nettskjema, we wanted to analyze possible correlations between some of the questions. We downloaded the survey results as a txt-file and imported this into IBM SPSS Statistics to generate correlations. We had three options of correlation analysis; Pearson's, Kendall's and Spearman's. Zinda (2021) writes about the main differences between these three methods, and that formed the basis for our decision. Pearson's measures a linear relationship between two variables, which assumes that the variables move together at a constant rate. One can think of this as a straight line. Kendall's and Spearman's measure the monotonic relationship, meaning that they measure how likely two variables are to move in the same direction, but not necessarily at a constant rate. In our analysis, the rate of y changes varies at different values of x, indicating that we should use Kendall's or Spearman's. They are both non-parametric, i.e. the two variables do not have to fall into a bell curve. Kendall's are more robust and are generally the most preferred method. Kendall's work with both continuous data (i.e. ranked) and ordinal data (i.e. non-continuous data), while Spearman's work only with ranked data. Based on the above specifications, we decided to use Kendall's to analyze for correlations in the survey.

We translated all text answers from the survey into numbers and did a bivariate correlation analysis using Kendall's rank correlation. This resulted in a matrix consisting of all connections between answers. The correlation coefficient between two variables will return a value between -1 and 1. The further the value is from 0 the stronger the relationship. -1 being a strictly negative monotonic relationship, meaning that variables are inversely related, i.e. when one variable increases the other decreases. 1 being a strictly positive monotonic relationship, meaning that when one variable increases, the other also increases, and 0 representing no relationship. In instances where the score falls within the range, there exists a relational tendency, indicating that the correlation may not necessarily hold true for all cases, but becomes increasingly probable as the score increases. In our result analysis, we undertook the task of translating the numerical correlations back into text answers provided in the survey. This was done to ensure that our analysis was comprehensible for all readers. E.g. if we wanted to analyze the correlation between the app being easy to use and employees finding the app frustrating, we numbered the answers with "strongly disagree" as 1, "disagree" as 2, "neutral" as 3, "agree" as 4 and "strongly agree" as 5. When one variable increased, we could then easily watch what happened to the other variable. As researchers, we shall merely present the correlation coefficients, without providing any explanations as to why these correlations may have occurred. Moreover, the correlations are mutual in nature, and each coefficient are presented only once.

3.5.2 Qualitative Analysis

For the qualitative data derived from the interviews and the textual answers in the survey, Tjora (2019) suggests an inductive empirically close coding strategy. This is a ground-up strategy, where the codes are extracted from the data, without preconceived notions of what the codes should be. Thus, it is possible to reduce the influence of presumptions and theories, and hence avoid jumping to conclusions on the basis of "gut-feeling", Tjora (2019) explains. Also, the close grounding in empirical data means using terms already present in the data. The point is that the codes should correspond closely to interview statements and should capture the specific nature of the material (Tjora, 2019). This approach is well-suited for UX-research that desires to encapsulate some very human, subjective experiences and feelings. Also, as we are very familiar with 2FA in M365 in our everyday lives, an inductive approach may prevent researcher biases.

We did a complete transcription of each interview, based on the recordings, as suggested by Tjora (2019). This was to document every statement by the interviewees in their own words. The transcripts were written the day of or the day after the interviews had taken place, in order to preserve personal impressions about non-verbal cues and the interview setting. Though the interviews were transcribed according to the letter, local dialects of the interviewees were translated to formal Norwegian, which also acts as an anonymization of the individuals (Tjora, 2019). All quotes were translated to English for this thesis.

In the conceptualization stage of the data analysis, theoretical perspectives were combined with the empirical material to develop relevant and justified concepts (Tjora, 2019).

We used Taguette to analyze the qualitative data. This program enabled us to collaborate in making tags, i.e. codes, to see similarities and differences between the interviews. We started out by importing the transcribed interviews into the program. We then started to analyze the interviews and we created tags based closely on subjects from the interview statements. We already had the interview guide in the back of our minds during this phase, and it formed a basis for some of the tags. When we started analyzing, we could highlight words or sentences from all the interviews and connect them to one or more of the self-created tags (see appendix E.1 for the interview codes and appendix E.2 for codes from the textual answers in the survey). Given the functionality of Taguette, the tags relate more to what Tjora (2019) describes as sorting-based coding, i.e. when codes are sortable subjects, whereas each subject features a respective contextual description (qualitative value). Still, Taguette would create a list of all the empirical statements marked the specific code, and what interview the quote originated from. So in practicality, this resulted in a list of empirically close codes.

During the course of the interviews, one of the questions pertained to the specific qualities of employees that are deemed essential for creating a good IT security culture. This question resulted in a code called "qualities of employees". We could easily navigate to this code and see all the answers containing different qualities of employees. We both analyzed all interviews, making sure no valuable information was omitted. Later, all tags could be viewed separately, or several together, to discover which interviewees had made similar statements.

3.5.3 Mixed Methods Analysis

In our research we have used both quantitative and qualitative methods, but with a common purpose to generate results for the same research question. Combining data collecting methods and thereby mixed methods data analysis, offers several advantages, Oates et al. (2022) explains. Firstly, it enables us to study the research phenomenon from several perspectives and detect nuances. Secondly, it allows for findings to be confirmed, supported or questioned by data from another method. This aligns with the concept of data triangulation, as explained later in section 3.6.2. After analyzing the data separately, the data must be integrated to draw comprehensive conclusions.

Surveys, as a quantitative method, are meant to gather large amounts of data, which makes it difficult to get detailed answers. Although we provided the respondents with an "other" option, they typically did not provide detailed responses in such cases. We wished to conduct the survey prior to the interviews to analyze the survey and use the survey answers as a base for the interview questions. We discovered that many respondents wrote their own answers to especially two questions. This was the question asking if they experience challenges with 2FA and the question asking what their motivation for using 2FA is. These questions had multi-answer checkboxes and the possibility of writing something entirely different. Consequently, we chose to include these questions in the interview guide, since respondents evidently had a lot of reflections they wished to express about these topics, and we needed to discover this in more detail in the interviews. The level of detail from the qualitative material is the reason why the interviews are given the greatest emphasis.

3.6 Quality of the Research

The quality of the research and the findings are a result of the decisions made in regard to all the phases in the method. Tjora (2019) describes the three established criteria used to measure quality; reliability, validity and generalizability. These measures are frequently a point of criticism of case studies (Quintão et al., 2020). In the following paragraphs an attempt is made to describe these conditions and what we have done to ensure that they are upheld throughout the thesis.

3.6.1 Reliability

Reliability is a measure of the internal logic or consistency throughout the research project (Tjora, 2019). Tjora (2019) writes that reliability is strengthened by communicating how decisions in the study are made in accordance with academic principles. This can e.g. concern the actors involved and their relationships - like the one between researcher and participant. Additionally, the researchers' involvement in the studied topics are of importance and how their position, commitment, knowledge and experience will influence the analyzing and discussion of the results (Tjora, 2019).

To strengthen the reliability of this thesis, there has been a great emphasis on describing the methodology, design decisions and the background for the case. Even though a completely objective researcher is desired in research, it is seldom completely obtainable in practice (Tjora, 2019). For that reason, we have, after the best of our abilities, researched without preconceived notions or specific expectations for the results. For example, the selection of interviewees was made neither by us nor our contact person in Atea, based on personal convictions. The selection was done by the HR manager in Atea, with no other attachments to the research project, and were given no instructions on who to select.

Still, it is reasonable to believe that our previous personal experiences and perceptions regarding the matter have affected our outlook on the literature, the survey and the interviews. As an example, it is possible that while the interview guide used in the study was designed to avoid leading questions, the follow-up questions asked during the actual interviews may have unintentionally included leading language or implied a preferred response. It is possible that these biases resulted from a lack of training or experience as interviewers, posing in-depth questions that may have implied a preferred response, or feeling compelled to clarify the intention of the question to the interviewee. This can result in potential biases in the data collected, as participants may feel pressured to answer in a certain way or may inadvertently provide responses that align with our expectations. It is essential for us to be aware of these possibilities and take measures to mitigate any potential biases in the research process. Tjora (2019) maintains that this represents a disturbance in the project, and may consequently affect the final results. It may have prompted the interviewees to express or emphasize something they otherwise would not particularly consider.

3.6.2 Validity

Validity is concerned with the logical consistency between the project's research design and its findings, and the research questions to which answers are being sought (Tjora, 2019). Tjora (2019) argues that validity is mainly strengthened when it is tested in dialogue with the research community, i.e. constantly comparing and relating the findings to previous research and current theories and perspectives. To ensure the validity in a case study specifically, multiple sources of evidence should be used and also a process of triangulation of data (a variety of data sources or methods, including time, space and people) (Oates et al., 2022; Quintão et al., 2020; Yin, 2009). This is especially important for the quality of the data and its treatment and the research methodological rigor, as case studies are not generally possible to replicate (Quintão et al., 2020). Furthermore, the authors suggest review of the reports from the interviews and a defined logical chain of events in the research, which is important to provide information to the readers about the project process that leads to the conclusions.

Being transparent about the research process, the methods and the choices might also strengthen validity (Tjora, 2019). In the planning of the research design we made use of several acknowledged sources on methodology to make informed decisions throughout the process. The angle of the study was shaped by the findings made in the interviews compared with answers from the survey and theory from relevant literature. The literature mainly included articles covering both breadth and depth of our topic and research question. Some literatures were articles with very similar research questions like ours, while others discussed more general topics like security, UX and culture - contextualizing our research question.

One weakness to the study may be the lack of data triangulation both with the survey and the interviews. This was mainly limited by practical considerations of the research project as a master thesis of this scope. In this case, we initially intended to study users of M365 among the clients of Atea to increase the diversity of the sample and provide data triangulation. However, due to difficulties in conducting this in a methodologically sound way, we opted to limit the research to in-house at Atea. We instead incorporated a question in the interview guide where the interviewees had a chance to share their experiences of these topics working with customers. Though a few had this specific experience or expertise working as consultants in End-User Computing, most of the interviewees could not report about their customers' user experience of 2FA in M365.

3.6.3 Generalizability

Generalizability describes the relevance of the research beyond the examined case (Jacobsen, 2005; Tjora, 2019). Generalizability requires a representative sample in relation to the population one wishes to generalize to (Jacobsen, 2005). Case studies as a method are often criticized with the argument that their findings are less generalizable (Oates et al., 2022; Tsang, 2014). Since M365 as a tool and 2FA as a security mechanism are widely used across organizations and industries, it would be highly useful and desirable to be able to generalize the results from our research. Oates et al. (2022) explain how this is possible even with case studies, as some factors in the case can typically be found in other cases as well. Therefore, generalizations can be made to the extent that the case in question is typical for other cases.

On one hand, by combining both survey and interview methods, we were able to collect extensive and diverse data from a range of sources, including consultants and in-house employees. The survey achieved a relatively high response rate (i.e. approximately 35%), and after conducting nine interviews, we observed a high level of consistency in the responses, which is a positive indicator of the sample size. Furthermore, Atea's use of 2FA and M365 in their internal systems is not unique, but rather typical of many Norwegian and Nordic IT consultancy firms of similar size and organizational structure.

On the other hand, all informants work in the same IT firm, where we can assume there is a larger focus and awareness regarding these issues than in many other organizations. It would have been interesting to study their customers, specifically employees not working in IT businesses, such as those in health care or municipal sectors. Additionally, interviewing individuals from a more diverse range of hierarchical positions within Atea, including managers at all levels, could provide further valuable insights into the perspectives of organizational leaders on these issues.

3.7 Research Ethics

3.7.1 The Importance of Research Ethics

In our research we study people; what they think, what they do and how they do it. Several authors note that this can be perceived as a kind of intrusion to their lives and their sphere (Jacobsen, 2005; Tjora, 2019). Therefore, as researchers, we are expected to make some ethical considerations in advance, so that we can meet ethical dilemmas along the way in the research process with reflected choices based on ethical principles (Jacobsen, 2005).

One aspect to consider is the relationship between researcher and participant (Jacobsen, 2005; Oates et al., 2022). Important aspects such as trust, confidentiality, respect and reciprocity affect our relationship with other humans (Oates et al., 2022; Tjora, 2019). As researchers we need to be aware of how we behave and communicate with the participants to establish these aspects in the relationship. All informants to the interviews participated voluntarily and made an informed consent with the right to withdraw at any point. All collected data have been anonymized, so that no individual is identifiable. All data has also been stored in safe folders on computers throughout the research.

Another relationship to be aware of is the one between researcher and the external company (Jacobsen, 2005). Such collaboration places high demands on the researcher's integrity. It is particularly important that the researcher does not carry out investigations and avoid using methodological knowledge to lead to a particularly desired and beneficial result for the company (Jacobsen, 2005). In our case, Atea is a company outside NTNU that we are collaborating with. We contacted Atea in the early stages of our project report, which was written the semester prior to our master thesis. Atea invited us to a meeting and presented us with some possible topics for a potential collaboration for a master thesis. Next, we wrote a motivation letter that led to the formalization of the collaboration. Together with Atea and our supervisor, we came up with the exact formulation of our research question within the topic. An agreement was signed by the researchers, Atea and NTNU to ensure a level of professionalism and establish the respective rights to each party involved. An oral agreement was made during an early information meeting to confirm what Atea could provide for us for the research. This included practical aspects, such as using their offices a few days a week during the project. During our time at Atea we also held two presentations about our research and findings, but after the end of the project, we had no further obligations to Atea.

3.7.2 Reporting to NSD

In Norway, it is mandatory to register all research projects that involve processing of personal data to NSD (Jacobsen, 2005) (now a part of Sikt (Norwegian Agency for Shared Services in Education and Research))(NSD, 2021). The EU's (2016) GDPR defines personal data as "any information relating to an identified or identifiable natural person [...]" (p. 33). In our data collection methods, specifically the interviews, this may include data such as age and gender. Before conducting the data collecting, we therefore applied our research project to NSD. The research project was approved, and was carried out in accordance to how it was described in the application (see appendix A).

3.7.3 Ethical Considerations regarding Interviews

It was highly prioritized that the interviewees voluntarily consented to the interviews fully informed. Further, they should get a sense of safety and respect during the entirety of the interview process. Jacobsen (2005) notes that it is ideal for interviewees to have a complete understanding of the information being discussed during interviews, but acknowledges that it may be challenging for researchers to ensure this. We repeated the information in the consent form orally (see appendix B) when conducting the interviews, and asked for their consent to record and transcribe the audio or video.

3.7.4 Weaknesses with the Data Collection

The collected data will be used to draw conclusions applicable to Atea, however it should be noted that in order to generalize with a high level of certainty, several responses from a population are typically required. We collected 122 answers to the survey, which is a satisfactory amount out of the 350 in Region Nord that received the participation email. Still, a possible weakness is that, given that it is a voluntary survey, respondents with strong or distinctive opinions may be more likely to participate, while those who have less defined opinions may choose not to participate.

Surveys usually receive a large number of respondents, making it time consuming to analyze only short text answers. Since the survey was not our primary method of collecting data, we chose to provide answer options to all questions, making it more efficient in analyzing a substantial amount of data. Some of the questions still had options for "other" so that respondents could enter answers manually. This was done not to limit the responses to only our proposed options, if respondents had other valuable insights. When answering a question with answer options, respondents could easily just choose some answers without carefully considering the question. When we asked "Are you experiencing any challenges with two-factor authentication at work?" and provided them with a few different challenges, there might be challenges that we unintentionally neglected, and that respondents did not take their time to consider, since they were already presented with other options. This is a weakness with surveys in general, making it difficult to know if all possible answers have been collected.

In the survey we asked whether or not they agree with receiving adequate training in 2FA. It is a weakness that the formulation of the question never made us aware of the amount of training, only if employees were satisfied. Several employees were not satisfied with the training, and we should have known how much they actually receive.

The shortest time a respondent spent in answering the survey was 1 minute and 48 seconds. We cannot say anything about the validity of the answers, but when such a short time is used, one may question the thoroughness of the answers. There are cases in which people do not read the questions in a survey, they just answer arbitrarily. This is one of the reasons why surveys are not as reliable as interviews. The validity could have been improved by adding questions to ensure that respondents paid attention to the survey. Such a question could be "what is 2+4?", which is simple, and everyone should be able to provide an accurate answer. We chose not to do this, to limit the time it would take to answer the survey. Since the survey was voluntary, we assume that most respondents wanted to answer the survey, and therefore answered honestly - not just arbitrarily selecting options.

When asking questions with multi-answer options, like at the end of the survey, each respondent could tick multiple answers, yielding the total answers exceeding 100%. Many respondents have ticked "other" on questions like "Are you experiencing any challenges with two-factor authentication?", and wrote their own answers, which are actually just elaborations of the presented answer options. We must keep this in mind when analyzing the percentage of respondents choosing "other" instead of choosing a specific option.

It might also be a weakness in the survey that we did not ask whether they are a manager or not. We are unsure if this could be relevant in regard to their knowledge of IT security. Forgetting to ask a question is a weakness, as there was no way for us to contact an employees' response in the survey later on. In contrast, numerous interviewees told us to contact them if we had more questions, even if that turned out not to be the case. Still, we knew that there was a possibility to contact interviewees at a later point, on the contrary to contacting respondents from the survey.

We only conducted nine interviews. Even though we both analyzed the transcribed interviews in Taguette, there might be important statements and quotes from the interviewees that we missed or misinterpreted. As researchers, we still did our best to be objective when analyzing the interviews.

4 Results

The results will comprise of three primary sections; the first containing quantitative and qualitative analysis of the survey, the second containing qualitative analysis of the interviews and the last containing a comparison of these results. The questions from the survey and the questions asked in the interviews can be seen in appendix F and C, respectively. We will categorize the results of the survey and analyze them accordingly. Similarly, the findings from the interviews section will be presented in a categorical manner. The presented data in the results chapter will form the basis for further discussion with theory in the next chapter.

4.1 Quantitative and Qualitative Analysis of the Survey

We received 122 answers on the survey from 350 possible employees, which is a response rate of approximately 35%. As specified in section 3.4.1.2, the survey was conducted in four distinct sections, each of which the respondents were required to navigate through. In the survey, there were a total of four questions that elicited qualitative responses. These were open-ended questions that were supplementary to the multiple-choice questions, allowing the respondents to provide textual answers beyond the options provided. One question aimed to gather the respondents' preference for 2FA-methods, while two other questions focused on identifying what challenges the respondents experience using 2FA. There was also one question about the respondents' motivation for using 2FA, however it should be noted that this question received only one answer. The textual answers were analyzed in their entirety, and 22 codes were generated using empirical close coding (see table E.2 in appendix E).

In this section, we will first present demographics and background information about the respondents. Next, the topics will be presented aligning with the research questions; (1) the user experience of 2FA in general, before we look closer at the Microsoft Authenticator App, as it is the primary 2FA method used, (2) the three main challenges the respondents experienced are identified through both quantitative and qualitative analysis, and (3) we report from the findings regarding the cybersecurity culture of the organization, and how this potentially relates to the user experience of 2FA, according to the respondents. After a summary, a correlation analysis is done.

4.1.1 Demographics and Background Information

Included in the survey were some questions to outline some demographic information deemed potentially relevant to the results. With regard to the age of the respondents, the distribution was quite even, as can be seen from figure 4.1. Most of the respondents, 29.5%, were between the ages of 20-29. The age groups 30-39 and 40-49 were almost the same size, at respectively 23% and 22.1%. 13.9% of the respondents reported to be 50-59 years old. Lastly, the smallest group of 11.5% reported to be 60 years and older. The gender distribution shows a large majority of males, i.e. 79.5%, and a minority of females, only 20.5%. This can be seen from figure 4.2.

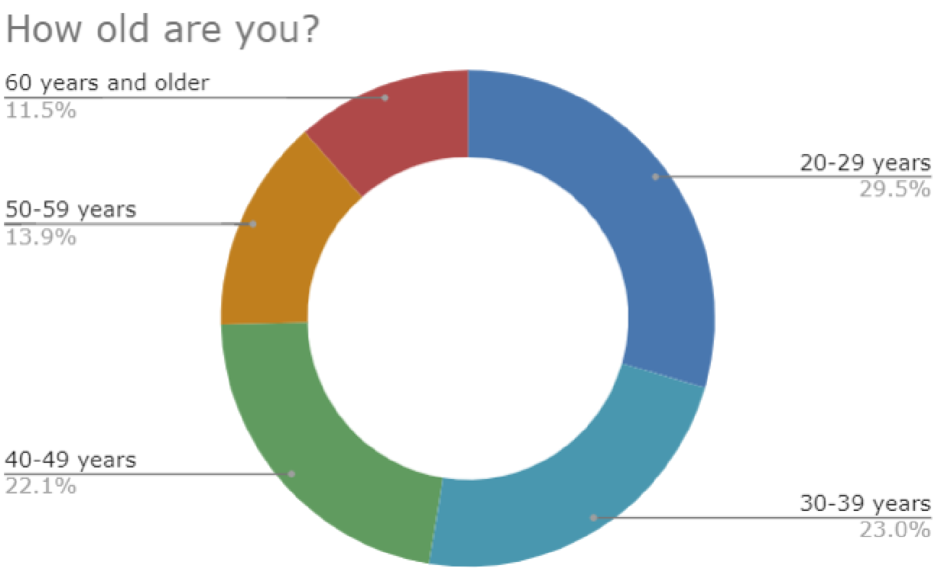


Figure 4.1 Age distribution from the survey.

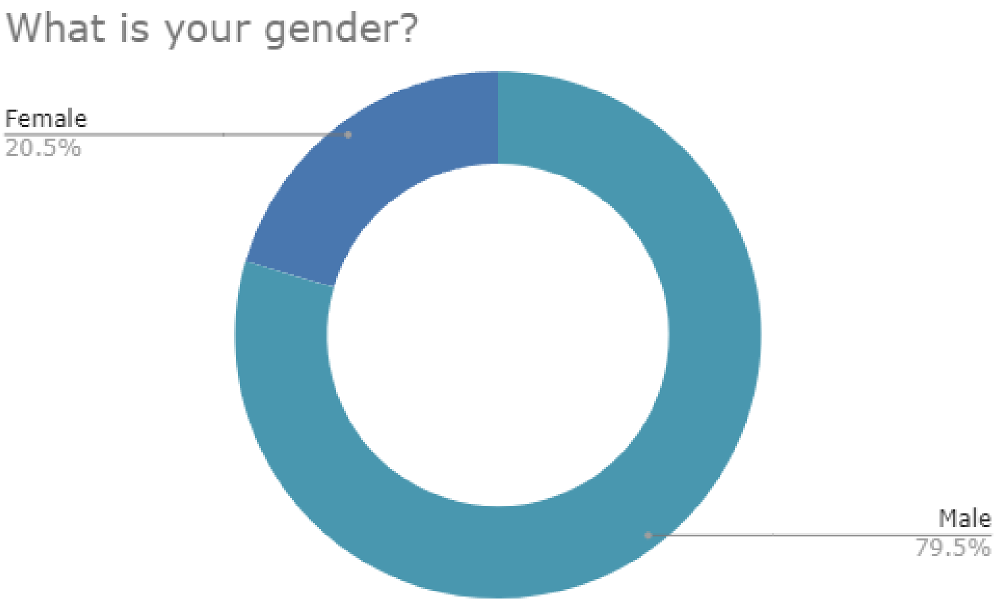


Figure 4.2 Gender distribution from the survey.

Subsequently, the survey inquired about the participants' general background and experience to gauge their perspective and level of expertise in cybersecurity. Firstly, the respondents were asked what department of Atea they work in (see figure 4.3). There were five broad answer options provided to the respondents, according to information from our contact person in Atea. Consequently, the answers do not properly convey the competencies of the respondents, but makes it possible to see potential relational tendencies. Approximately half of the respondents, 50.8%, work as consultants. That is, they provide professional advice and expertise to the customers of Atea. What role they have beyond this, e.g. if they are technical or non-technical consultants, is not specified from the answers. Next, 16.4% of the respondents work in Atea Managed Services, meaning that they are responsible for the IT-processes and -functions of the customer. In total, 28.7% reported to work in sales; specifically 15.6% in solution sales and 13.1% in regular sales. Lastly, 4.1% reported to work within administration and management.

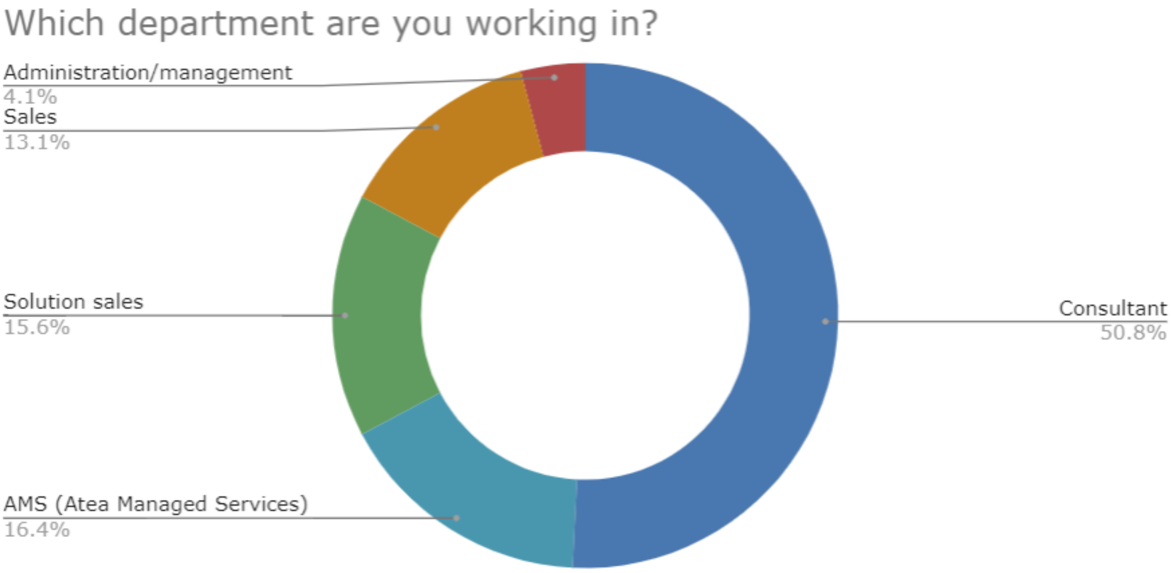


Figure 4.3 Distribution of which department the respondents of the survey worked in.

4.1.2 User Experience of Two-Factor Authentication

4.1.2.1 Preferences for Two-Factor Authentication Methods and Factors

The respondents were asked if they use the Microsoft Authenticator App (figure 4.4). The large majority, in total 91.8%, reported that they use the app to some extent, i.e. 34.4% reporting usually using this method, and 57.4% reporting often using other methods. Only 8.2% reported that they do not use the app at all. Additionally, the respondents were asked what their preferred method of 2FA is at work, as depicted in figure 4.5. The majority of respondents, 64.8%, stated that they prefer the Microsoft Authenticator App as opposed to receiving an SMS (23.8%) or a phone call with a numeric code (0%). A small proportion, 5.7%, do not have a preferred way of authentication. Another 5.7% of the respondents specified other answers than the ones provided, which is reported in the next paragraph.

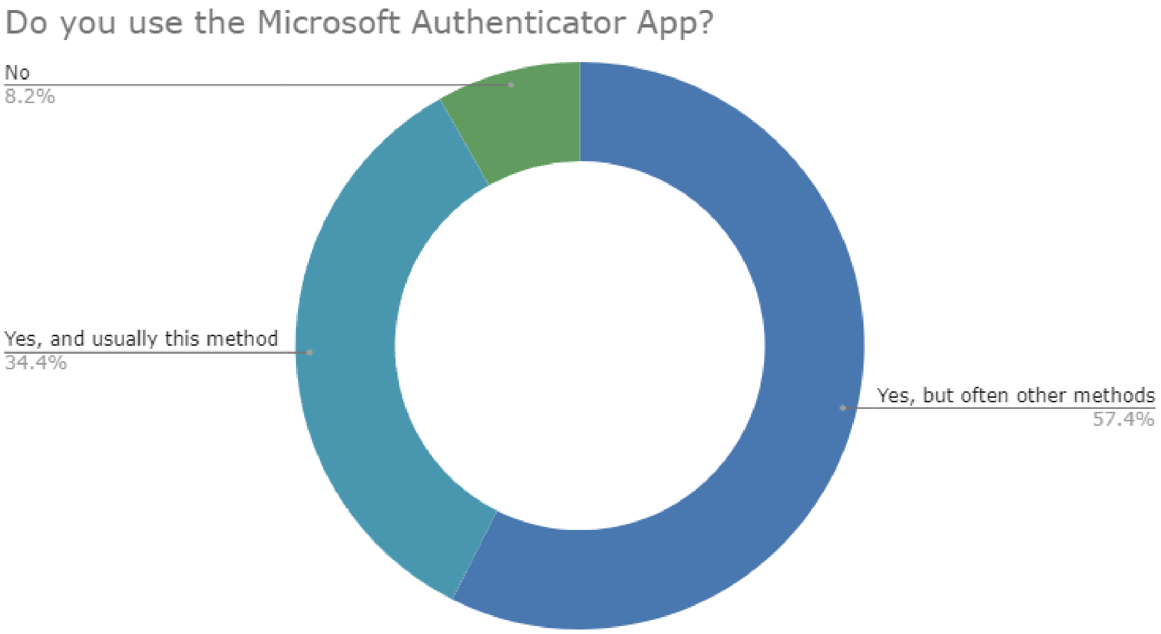


Figure 4.4 Distribution of usage of the Microsoft Authenticator App.

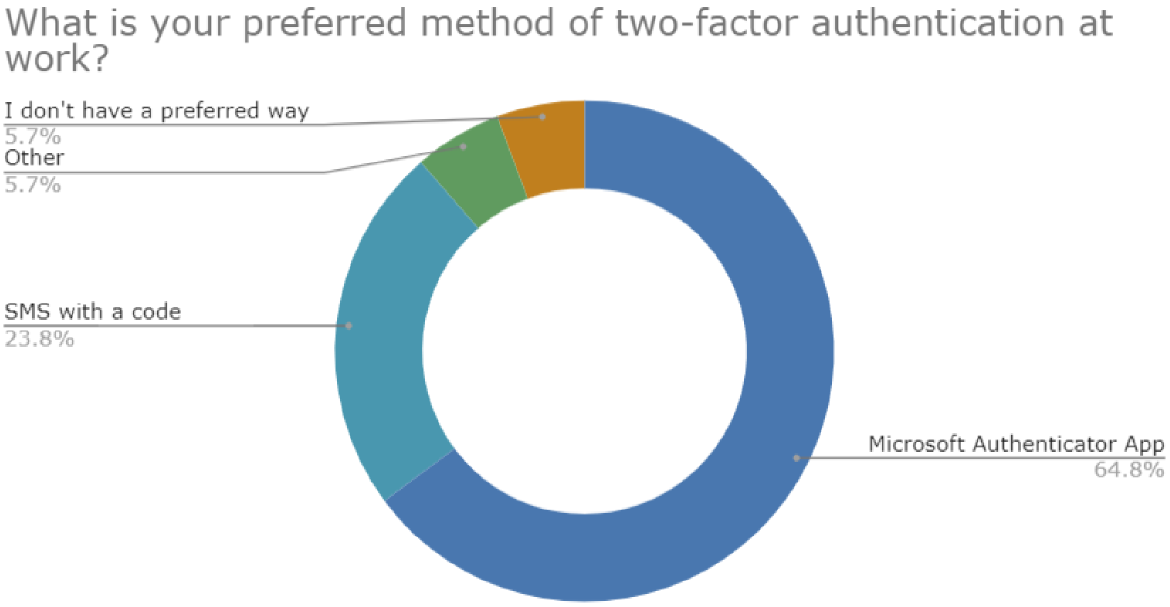


Figure 4.5 Distribution of the respondents' preferred method for two-factor authentication at work.

When referring to types of factors they prefer, there are particular two types that are commonly repeated in the textual answers. Biometric factors and physical tokens are equally many times addressed as their preferred methods. More specifically, several respondents suggest that FIDO hardware keys should be implemented, which is a physical device used as the second factor in the authentication process (see section 2.3.3). The reasons for these preferences are not elaborated upon in the answers provided by the respondents. Another respondent wished to combine the use of the Microsoft Authenticator App with other factors.

"The implementation is old fashioned. We could use compliance and the PC as a second factor, so that the authenticator app is only used in unsecured situations." - survey respondent

The respondents were also asked to compare 2FA in M365 to 2FA in other digital tools, as seen in figure 4.6. About half of the respondents, 52.4%, experience the digital solutions as "about the same". In total, 34.5% of the respondents report on the experience in Microsoft being somewhat better than in other digital tools, i.e. "much better" with 11.5% and "slightly better" with 23%. On the other hand, 7.4% experience it as somewhat worse than in other digital solutions, with 3.3% and 4.1% as "slightly worse" and "much worse", respectively. 5.7% answered the question with "don't know/not relevant". If we exclude the respondents who answered "don't know/not relevant" and give the remaining answers a value from 1-5, with "much worse" being 1 and "much better" being 5, we obtain an average of 3.37. From this number, we can derive that respondents think the Microsoft Authenticator App is in the middle of "about the same" and "slightly better" than other 2FA tools.

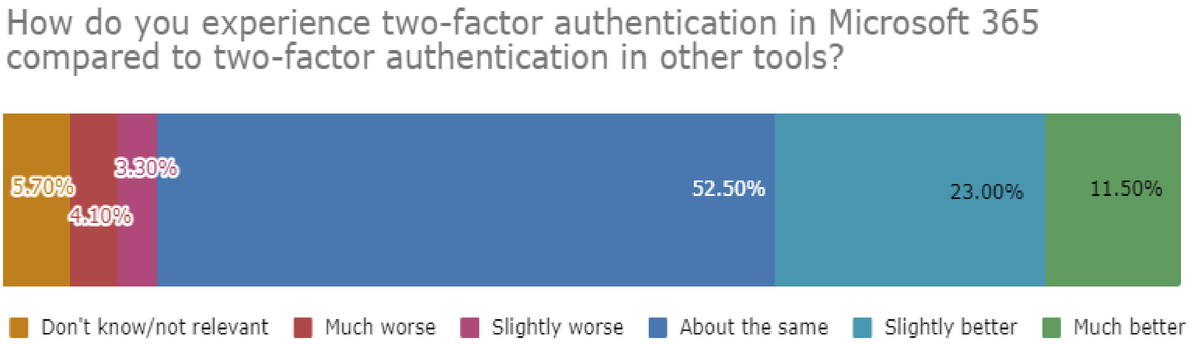


Figure 4.6 Comparison of two-factor authentication in Microsoft 365 and in other tools.

Furthermore, the respondents of the written answers expressed their preference for both Entrust and Google as providers of 2FA solutions. Following that the Microsoft Authenticator App was an option in the multiple-choice version of the question, it is not brought up as a preference in the textual answers, with the exception of one respondent writing that they wish they could always use the app, and not SMS. In some responses from other questions, the Microsoft Authenticator App was criticized and described as "hopeless" and "slow". We cannot say whether or not these responses were thought of in comparison to other 2FA tools, but they will nevertheless tell us how some employees perceive the app.

4.1.2.2 User Experience of the Microsoft Authenticator App

The respondents were also asked to give a rating from 1-5 on some statements mainly concerning the Microsoft Authenticator App. There were 10 out of 122 respondents in the survey that previously answered that they do not use the app. These respondents were therefore not given the below statements (figure 4.7) Each statement is vertically positioned on the y-axis and the scores from 1-5 are horizontally placed at the x-axis. The blue bars are visualizing the average score, i.e. the white number inside the bar. For example, when asked if the app is easy to use, the average score is 4.26, which one can see from the first statement in the figure, both from the number inside the bar, but also from the fact that the bar just crosses the line representing "4.00 Agree". From this we can observe that most respondents "agree" that the app is easy to use.

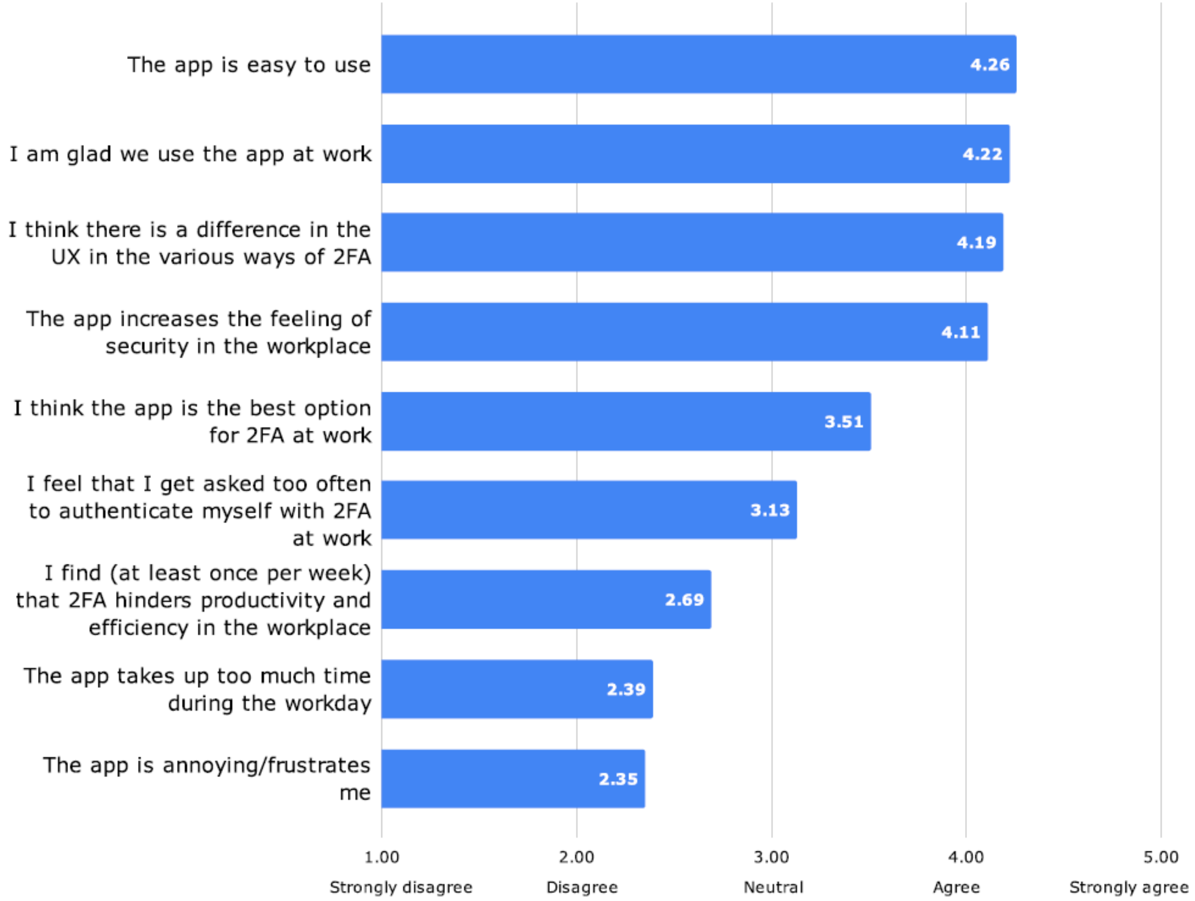


Figure 4.7 Graph visualizing average scores from statements regarding the Microsoft Authenticator App.

From figure 4.7 we can analyze that the respondents are generally glad that the app is used at Atea, with an average score of 4.22, as can be seen from the second statement in the figure. They also "agree" (average score 4.19) that there is a difference in the user experience in the various ways of 2FA and they "agree" that the app (average score 4.11) increases the feeling of security in the workplace. When asked if the app is the best option for two-factor authentication at work, the average score of 3.51 falls between "neutral" and "agree". The employees are "neutral" (average score 3.13) in regard to the statement concerning if they get asked too often to authenticate themself with 2FA at work. The next statement got an average score of 2.69 and falls short of "neutral". This statement asked if respondents find (at least once per week) that 2FA hinders productivity and efficiency in the workplace. Respondents "disagree" (average score 2.39) that the app takes up too much time during the workday and "disagree" (average score 2.35) that the app is annoying. More detailed numbers can be found in appendix D.

4.1.3 Challenges using Two-Factor Authentication

Figure 4.8 displays the responses gathered from the question that asked the respondents if they experience any challenges related to 2FA at work. A slight minority, 52 people, responded that they do not experience any challenges, while the majority, 70 out of 122 respondents, responded that they experience one or several challenges. After indicating that they face challenges, the respondents were presented with a follow-up question regarding the underlying reasons for these challenges, where they could select one or more reasons. Looking at the responses from both questions concerning challenges with 2FA, it is clear that these questions were interpreted similarly by the respondents. Since the consecutive question depended on the first, the question about *why* they experience challenges received 70 answers, versus 122 answers from the question regarding *what* challenges they experience. Reporting from the findings from these two questions in the next paragraphs, we have therefore combined the findings when analyzing, but maintained the graphs separate for answers to each question.

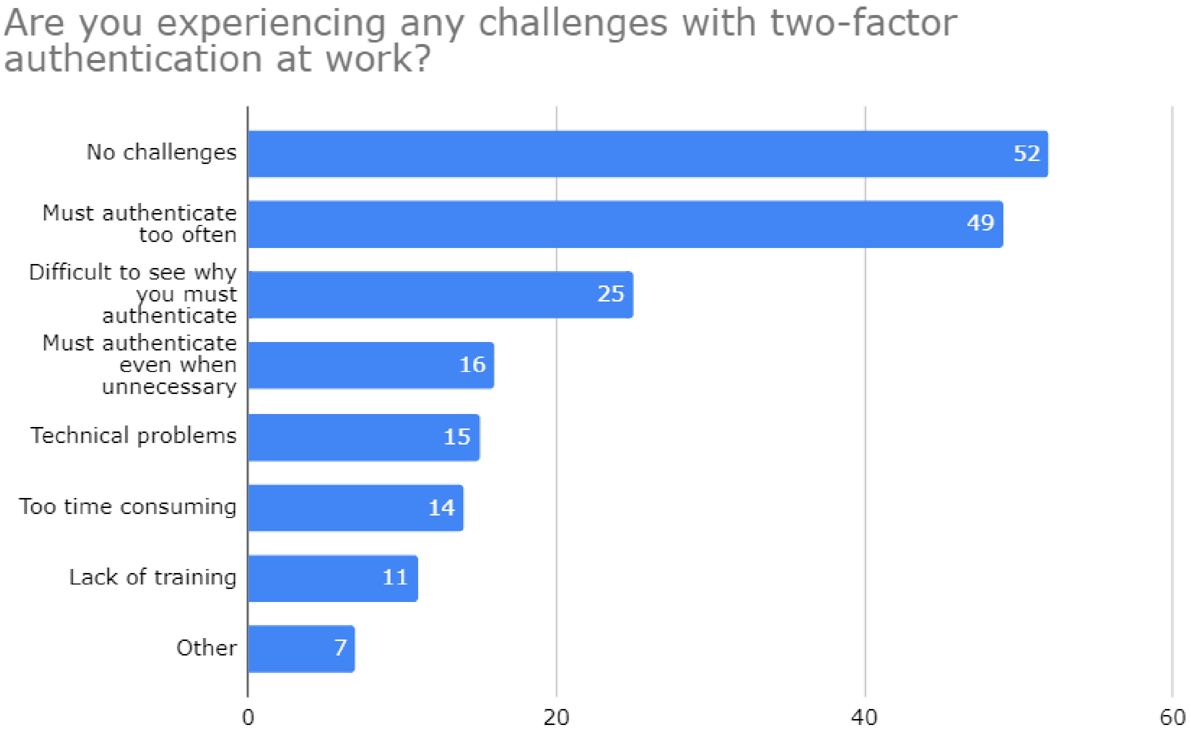


Figure 4.8 Different challenges experienced with two-factor authentication at Atea.

The respondents could select one or more challenges. The far most reported challenge, with 49 individual respondents agreeing, is frequency of authentication requests. Next, respectively 25 and 16 respondents find that it is difficult to understand the reasoning for the authentication request and the need for authentication even when it feels unnecessary. In the following paragraphs, we have combined these two statements into one challenge concerning illogical requests. Further, technical problems and the time it requires, are reported nearly equally many times each, respectively by 15 and 14 respondents. 11 respondents find the lack of training in 2FA as a challenge. 7 respondents choose "other", meaning they provided some textual answer to the question, which will be presented in the following sections. Summarizing the reported challenges, it can be analyzed that the central challenges users experience are the frequency of authentication requests, the lack of logic behind some requests and technical issues with the app. In the following paragraphs, these three challenges are further elaborated on.

4.1.3.1 Frequency of Authentication Requests

As mentioned in the above paragraph, the frequency of authentication requests during a workday is the most reported challenge. When asked about the frequency with which the respondents have to use two-factor authentication to access systems, the most common response, at 37.7%, is 2-3 times a day. This is shown in figure 4.9. The second most common response, at 28.7%, is 4-7 times a day. The rest of the answers are distributed from 12.3% reporting that they have to do it on average over 7 times a day to 4.1% reporting that they have to do the authentication less than once per day. 9.8% only have to authenticate approximately once per day and 7.4% reported that it varies a lot.

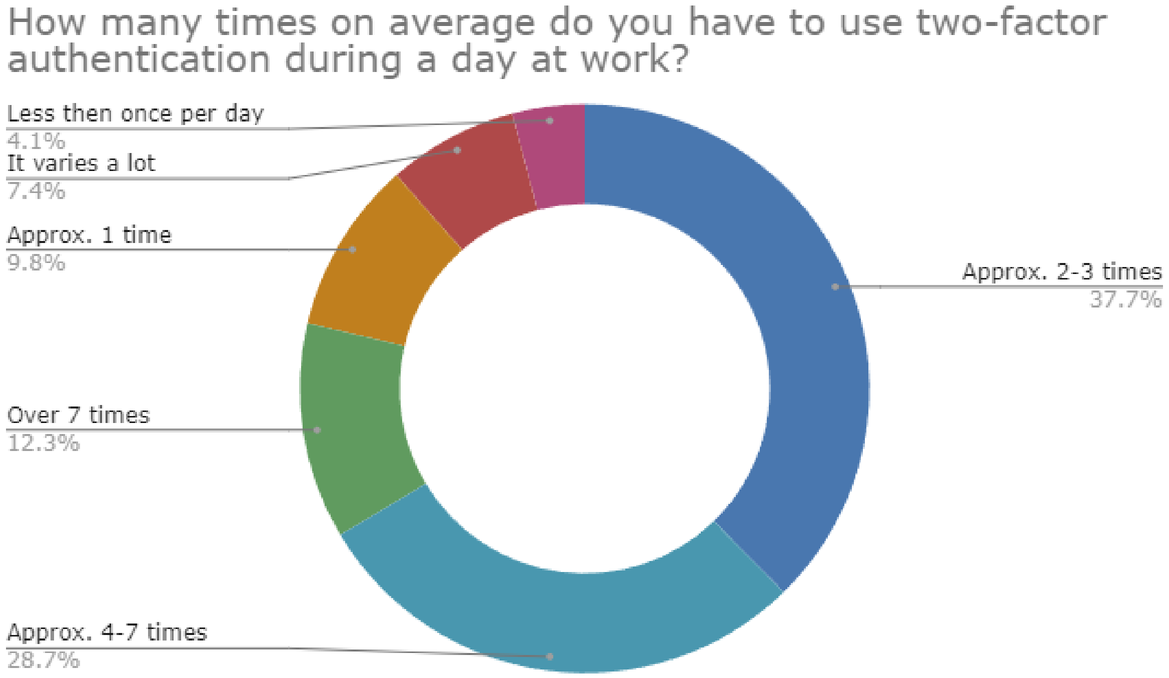


Figure 4.9 Distribution of how often employees must authenticate themselves during a day at work.

Also among the written answers, the respondents express that there are an excessive amount of requests to authenticate. One respondent specifically points out that there are too many SMS authentications. As one respondent writes, they are often asked to request multiple times right after each other, e.g. when opening multiple Microsoft applications.

"Two-factor authentication in Atea occurs far too many times during a day, and often right after each other when you start Outlook, Teams and Word. It should not be necessary to use MFA three times in 10 seconds in such situations." - survey respondent

Two respondents argue that one reason for the excessive authentication requests is the lack of SSO (single sign-on) integration across services. SSO is an authentication mechanism that allows users to gain access to multiple interconnected systems without re-entering their credentials.

"SSO [single sign-on] is not fully integrated across all services I depend on. The result is very many separate authentications during a workday." - survey respondent

Despite 49 people answering that they feel they need to authenticate too often, only 14 responded that the process takes too much time, as shown in figure 4.8. When asked *why* they experience challenges, 41 of the 70 respondents who experienced challenges agreed to "I am impatient" as a reason for why they experience challenges (figure 4.10). A fewer number of respondents, i.e. 12, agreed with the statement "2FA does not fit into my busy everyday life". 21 of the respondents in figure 4.10 answered "other", and several of the reasons they provided are included in this analysis according to their topic.

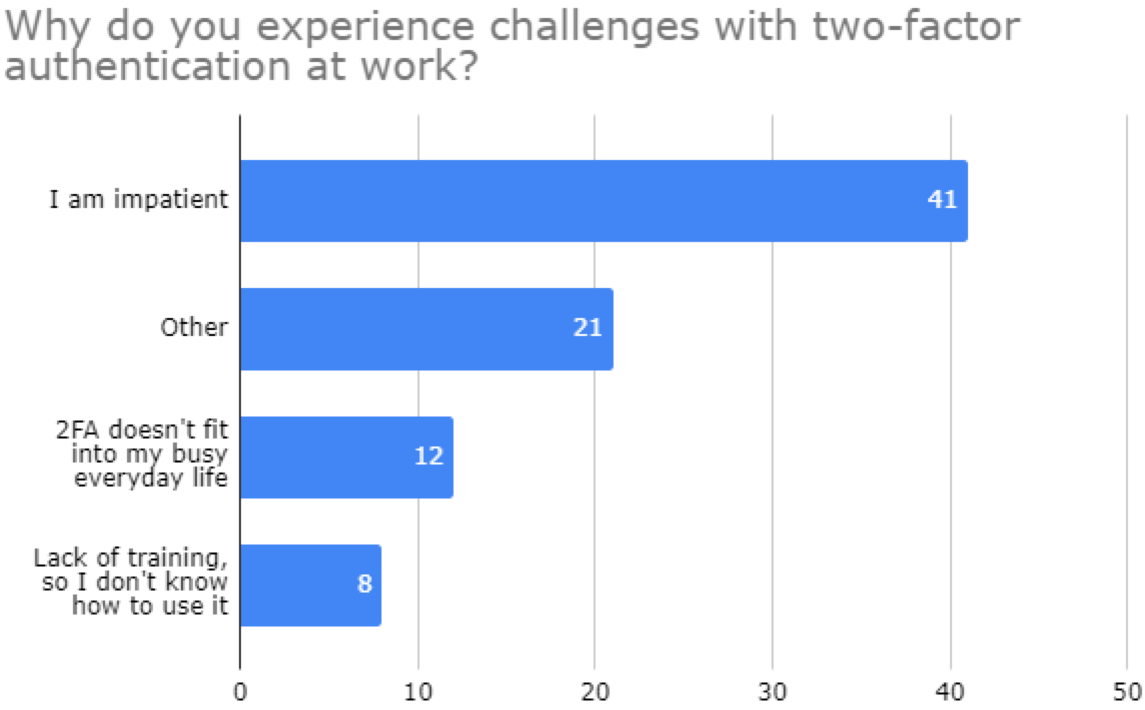


Figure 4.10 Why the employees experience challenges with two-factor authentication at work.

4.1.3.2 Illogical Authentication Requests

The second most reported challenge, according to 25 people (figure 4.8), is the difficulty in understanding why one is being asked to authenticate oneself in a given situation (e.g. that it feels arbitrary). Connected to this topic, one survey respondent wrote that they considered it a huge problem that there is no indication on the origin of the authentication request. Another respondent wrote:

"It comes at non-logical times. Not when starting the computer." - survey respondent

Somewhat similar to this statement, another option stated as a challenge that you need to authenticate yourself when you feel like it is not necessary (e.g. for login services without sensitive information). If a user experiences the authentication requests as not necessary in a given situation, it would also be an instance of feeling that the request is illogical. 16 respondents agreed with this statement (figure 4.8). For instance, one respondent experienced being requested to authenticate in the middle of a Teams meeting. One respondent expressed that this issue could be avoided if more policies were implemented to evade 2FA when unnecessary.

"There are too few policies implemented that prevent two-factor authentication when it is not necessary." - survey respondent

There is a possibility that the frequency of requests coupled with the lack of justification for them, could lead to uncritical thinking, as highlighted by two respondents. For instance, users could possibly approve fake or wrong authentication requests.

"You may also experience getting many requests when you log on to your computer from various [Microsoft] applications. It may lead to you just approving [the request] without actually knowing which login you're approving." - survey respondent

4.1.3.3 Errors During the Authentication Process

15 responded that a challenge is technical issues with the 2FA solutions (figure 4.8). Though this was not the most reported issue among the multiple-choice questions, technical problems were one of the most frequently brought up topics in the written answers.

Some respondents expressed concerns about the implementation of two-factor authentication within the organization. Certain respondents described the implementation as "old fashioned" and "inadequate". Another respondent attributed the problem to insufficient configuration of multi-factor authentication from Atea. In addition, one respondent also argues that they experience challenges because Atea's use of ADFS, and recommend that Atea end this practice (see section 2.3.3). Atea is in the process of moving systems into the cloud, but for the time being they still need the local domain servers to access SAP, which is their ERP-system (Enterprise Resource Planning). If these servers are down, authentication will fail. One respondent makes the connection from the current implementation of 2FA to the user experience.

"[2FA] is too poorly implemented in the job, [it] could be a much better user experience if it is set up correctly." - survey respondent

Another respondent reasons the technical issues due to the many different systems and inadequate SSO-implementation. The lack of proper SSO-implementation also explains the challenge described earlier of the frequency of authentication requests.

"Due to many systems and lack of SSO, but it is technically difficult to achieve with many systems from different suppliers." - survey respondent

Regarding specific, technical issues and their practical consequences, they are often caused by being disconnected from the internal network, causing the authentication not to be completed. One respondent points out how 2FA-notifications occasionally do not come through when the phone is connected to the guest network. Another respondent explained, as previously mentioned, how there is a specific problem when using Teams in M365.

"Experiences that [2FA] can come in the middle of a Teams meeting. The meeting works, but the Teams client stops, and the authentication dialogue box pops up behind the Teams application." - survey respondent

One of the respondents who also commonly experienced technical issues, noted that it is difficult to know why, because they have not received any training.

"Technical problems, such as the app not working. [But I] have received no training, so it may be that it is set up incorrectly or that I am using it incorrectly." - survey respondent

The survey was conducted before the number matching feature was implemented in the Microsoft Authenticator App. Interestingly, a respondent wrote that not typing in any numbers, i.e. only approving a request, was something they saw as a weakness, as it may lead to uncritical thinking, as previously mentioned.

4.1.4 Cybersecurity Awareness and Culture

On questions in the survey regarding the cybersecurity awareness and culture in the organization, the responses generally paint a positive picture. In the below figure (figure 4.11), the distribution of answers to these statements can be seen.

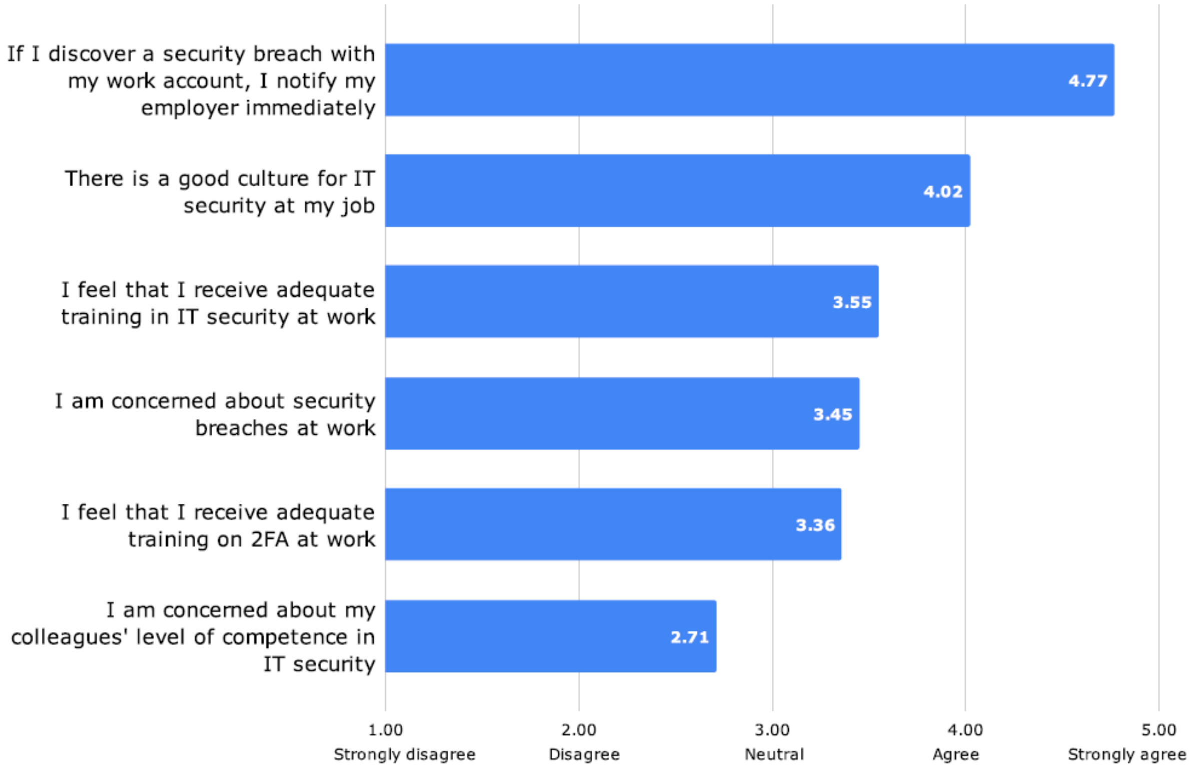


Figure 4.11 Graph visualizing average scores from statements regarding IT security.

The first statement in figure 4.11 discovered that respondents "strongly agree" (average score 4.77) in notifying the employer immediately if they discover a security breach at their work account. The employees "agree" (average score 4.02) that there is a good culture for IT security at Atea. They rate the level of adequate training in IT security at work as between "neutral" and "agree" (average score 3.55). The respondents are on average just over "neutral" (average score 3.45) concerned about security breaches at work. The level of adequate training on 2FA at work is closer to "neutral" (average score 3.36) than overall training in IT security, which was closer to "agree". The last statement in the figure asked whether or not the employees agree with concerns for their colleagues' level of competence in IT security. This average score of 2.71 falls between "disagree" and "neutral". These statements about the cybersecurity culture will be further elaborated on in the following paragraphs.

4.1.4.1 Motivations for using Two-Factor Authentication

When employees were asked about their motivations for using 2FA at work and were provided with multiple answer options, the large majority, 111 of the respondents, agreed to the statement "I know it is a safety benefit", as seen in figure 4.12. This aligns with the notion that will be explained later, that the respondents agree that they have an understanding of what 2FA is. A fewer number of respondents, 58 respondents, find the feeling of security being a motivation, with the statement "I feel more secure", which aligns with the fact that the respondents agree with the statement in figure 4.7 that the app increases the feeling of security. These two motivations are similar, yet not quite the same. While the first refers to the simple knowledge of a fact, the second describes a personal, internalized feeling.

67 respondents point at 2FA simply being a requirement as a motivation, agreeing with the statement "Atea requires it". Only one respondent did not know what their motivation to

use 2FA is. One respondent answered "other" and specified their motivating thought process.

"[I] sit with many users at customers who have access to all systems (administrators). Losing such an account can, in the worst case, mean bankruptcy for that business." - survey respondent

None of the survey respondents answered that they were not motivated to use 2FA.

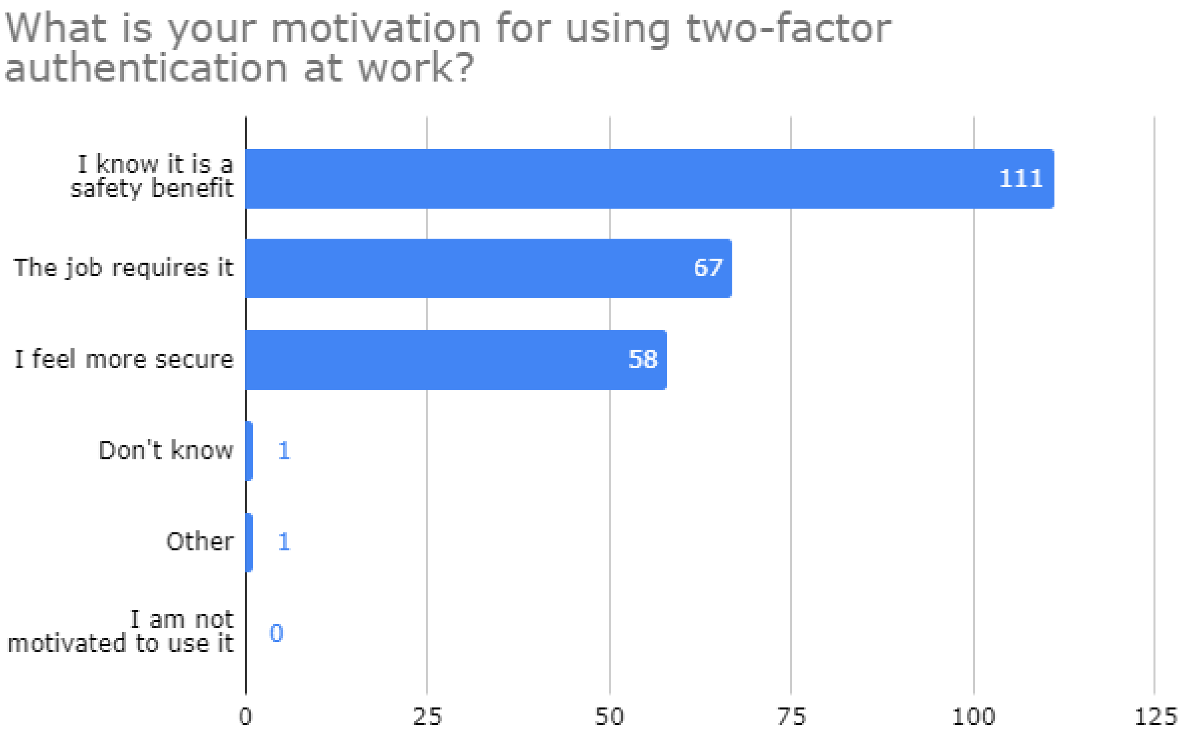


Figure 4.12 Motivations for using two-factor authentication at work.

4.1.4.2 Knowledge and Competencies

To map out the respondents' background, we included some questions in the survey regarding their competence in cybersecurity specifically.

Firstly, the respondents were asked "Do you work with security?", in that exact formulation (figure 4.13). It is therefore important to acknowledge that the question may have been interpreted differently, as it does not further specify in what way or to what extent we define "work with security". This prompt for a binary self-evaluation was not done to exploit intermediate shades of cybersecurity expertise in the data analysis, but rather to prioritize survey efficiency. Of the respondents, 53.3% answered that they work with security, while 43.4% answered that they do not work with security. 3.3% reported that they do not know whether or not they work with security. It is worth noting that this answer could be due to a different perception of what the question entails.

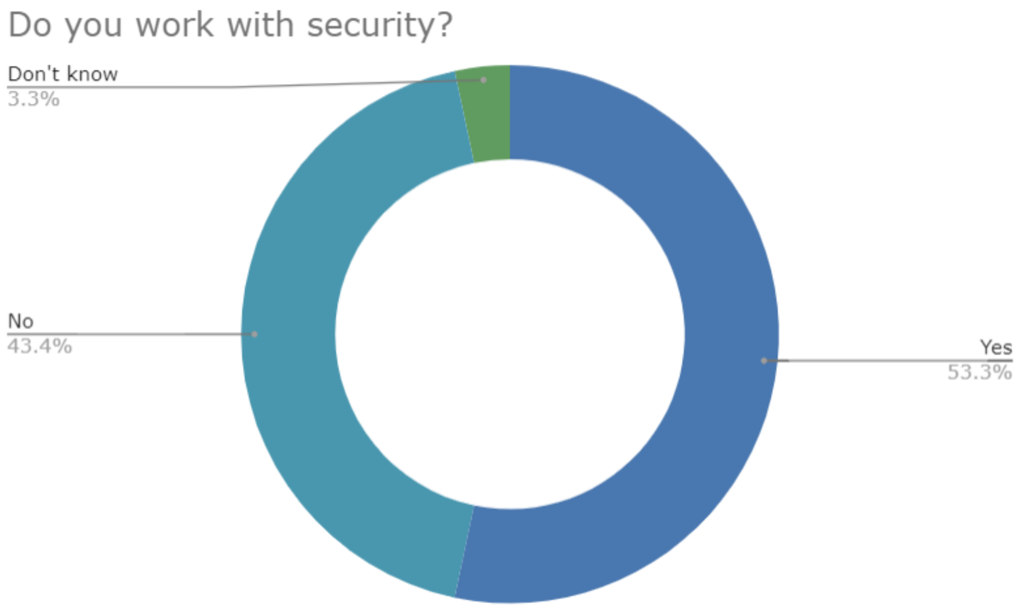


Figure 4.13 Distribution of employees working with security.

Separately, the next question asked respondents how they would rate their own competence in IT security on a scale from 0-10, where a higher score indicates a higher self-perceived competence, as can be seen from figure 4.14. The largest group of respondents, i.e. 27%, placed themselves at the middle score of 5, i.e. they perceive their IT-competence as neither poor nor good. In total, 67.2% placed themselves at a score between of 5 and 7. 8 and 9 were chosen by 18% of the respondents. 13.1% scored themselves between 2 and 4. 1.6%, i.e. two respondents, placed themselves at the highest score of 10, while no one placed themselves at the two lowest scores of 0 and 1. Overall, this results in the average being a score of 6.05.

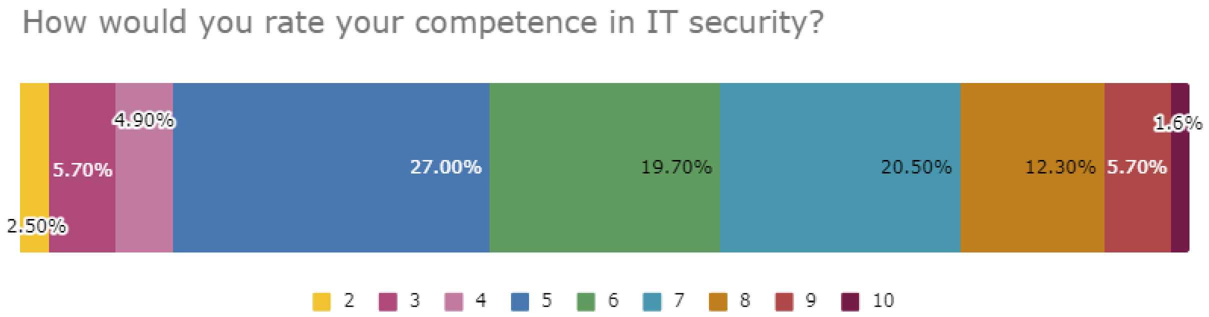


Figure 4.14 Distribution of respondents' rating of their own IT security competence.

If we look back on the question regarding challenges, 11 responded that the lack of training in 2FA is a challenge, seen in figure 4.8. We can connect this training to the cybersecurity culture of Atea. Similarly, when asked why they experience challenges with 2FA (figure 4.10), 8 of the respondents that experience challenges agreed with the statement "There is a lack of training, so I do not know how to use 2FA properly". As one respondent pointed out, the non-existence of training combined with technical issues makes it difficult to know where the issues lie.

Further, the respondents were asked if they have an understanding of what 2FA is, which can be seen from figure 4.15. Close to everyone, at 98.4%, answered "Yes". The remaining

1.6% answered "Partly". The answer options "No" and "Not sure" did not receive any answers.

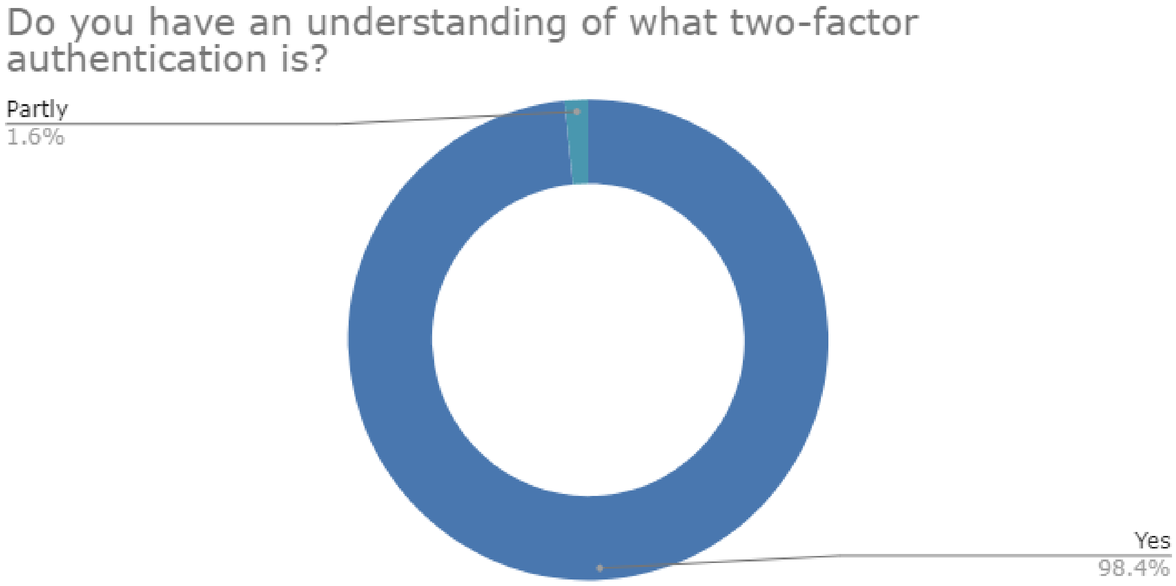


Figure 4.15 Distribution of employees' understanding of two-factor authentication.

4.1.5 Summary of the Survey

Summing up the responses, we see that the average respondent finds the Microsoft Authenticator App usable, and are satisfied with the security benefits 2FA provides. In fact, the minority do not experience any challenges of 2FA in their workday at all. However, the remaining respondents report several challenges to the user experience of how 2FA takes place in practice. Among these challenges, the most commonly reported is the high frequency of authentication requests. The second and third most reported challenge concern illogical authentication requests and technical issues. Regarding the culture for IT security in their workplace, the average respondent agrees that it is good. Despite experiencing these challenges, the respondents show high motivation for using 2FA, mostly because of the knowledge that it provides a security benefit.

Summing up the qualitative data from the survey, it is revealed that the questions regarding the challenges of 2FA were the most engaging among the respondents. There was a total of 29 unique textual answers to these two questions, while the one regarding 2FA method of choice received only 7. Concerning challenges, there was a predominance of more technical problems being addressed, with several respondents demonstrating a clear understanding of the underlying, technical issues. This may suggest that respondents with more technical competencies are more engaged by these questions, and are more inclined to provide elaborate responses.

4.1.6 Correlation Analysis

Upon conducting a bivariate correlation analysis on the responses gathered from the survey, we have discerned certain correlations of statistical significance.

We noticed that the statement "The app is easy to use" had the most correlations to other answers. This is not too surprising, because what respondents answered on other questions will most likely influence whether or not they find the app easy to use. It gives a coefficient of -0.236 in correlation to whether or not they work with security. If employees do work with security, they are more likely to agree that the app is easy to use. The coefficient of 0.306 indicates that when they find the app easier to use, the feeling of security in the app also increases. The more glad they are to use the app, the easier they also find it (coefficient of 0.471). Likewise, this assertion holds true if respondents hold the belief that the app is the best option for 2FA at work (coefficient of 0.368), i.e. the app is easier to use. When the app is easy to use, employees disagree that the app hinders efficiency in the workplace (coefficient of -0.183). Furthermore, if employees find the app easy to use, they are more concerned about their colleagues' level of competence in IT security (coefficient of 0.233). The easier the app is, the more employees agree in receiving adequate training in 2FA (coefficient of 0.161), whether or not they actually receive training.

Numerous correlations are associated with employees working in the realm of security. Employees not working with security have a higher probability of agreeing that the app can be annoying and frustrating, with a coefficient of 0.178. Additionally, if they do not work with security, they are more likely to disagree with concerns regarding security breaches at work (coefficient of -0.178) and with concerns regarding their colleagues' level of competence in IT security (coefficient of -0.287). Furthermore, employees who do not work with security tend to disagree with the notion that there is a difference in the user experience in the various ways one can use 2FA (coefficient of -0.164).

The coefficient of 0.254 indicates that males exhibit a higher likelihood of comprehending 2FA than females. However, this finding must be interpreted with caution since only two females out of 122 respondents answered *partly* on the question asking if they have an understanding of 2FA. Therefore, this result may not provide substantial information about the potential differences in understanding 2FA between males and females.

In the event of an increase in employees' rating of their IT security competency, the correlation coefficient of 0.155 indicates that they are more likely to agree to being concerned with security breaches in the workplace. This also implies an elevated level of concern about their colleagues' level of competence in IT security (coefficient of 0.307).

The survey statement pertaining to employees' potential frustration with the app usage displays several correlations. The first coefficient of -0.278 relates to which 2FA increases the feeling of security in the workplace. The greater the frustration, the weaker the feeling of being secure. Additionally, heightened frustration from the app also indicates that the app takes up too much time during the workday (coefficient of 0.522) and that employees feel that they must authenticate too often (coefficient of 0.345). The last two correlations to greater frustration suggest that employees find 2FA to hinder productivity and efficiency in the workplace (coefficient of 0.430) and that the Microsoft Authenticator App is worse than other tools for 2FA (coefficient of -0.282).

When the app increases the feeling of security in the workplace, numerous other statements or questions are affected. Respondents tend to disagree with the notion that the app takes up too much time (coefficient of -0.305) and disagree that the app hinders productivity and efficiency in the workplace (coefficient of -0.211). Greater feeling of security suggests that the Microsoft Authenticator App is better than other 2FA tools (coefficient of 0.307). Moreover, when employees perceive the app as more secure, they tend to report that they must authenticate themselves fewer times during the day (coefficient of -0.193).

Respondents indicating that the app is the best option for 2FA at work, do not find that the app takes up too much time (coefficient of -0.155) and disagree that there is a difference in the user experience of the various ways of 2FA (coefficient of -0.194). They also find that they must authenticate fewer times (coefficient of -0.201) when the app is the best option for 2FA. These correlation coefficients collectively suggest that the user experience of 2FA transcends the stand-alone usability of the application. It is noteworthy that there appears to be no observable reason for respondents who perceive the application as the best choice for 2FA to e.g. authenticate fewer times during a workday than those who prefer an alternative option, yet they still perceive a reduction in the frequency of 2FA.

It is probable that employees who acknowledge a difference in the user experience in the various ways of 2FA, disagree that there is a good culture for IT security at work (coefficient of -0.221). Furthermore, they may perceive that they must authenticate more often (coefficient of 0.228) when they experience a difference in the user experience.

There exists a higher probability that employees who express concern regarding their colleagues' level of competence in IT security, would experience an increased feeling of more frequent authentication (coefficient of 0.168).

4.2 Qualitative Analysis of the Interviews

The results in this section present the findings from the nine interviews with employees that were conducted over the course of two weeks. The findings are grouped in three main categories, based on our research questions: the user experience of 2FA, challenges of 2FA and cybersecurity culture.

4.2.1 User Experience of Two-Factor Authentication

4.2.1.1 User Experience of Two-Factor Authentication in General

For the most part, the employees interviewed had an adequate user experience of 2FA as a procedure in their daily work. Many found that the authentication process required limited attention, effort and time compared to the security benefits they know it provides. Negative user experiences were most often related to single instances, like the Microsoft Authenticator App malfunctioning or them being requested to authenticate too frequently in specific situations, either because of technical issues with the app, or other factors.

"I believe that in a perfect world, as I mentioned, I would have wished it to be easier. Even though it doesn't happen every day, it happens in certain situations. It's typically those situations where it's the least convenient, that you get the worst rush of authentication requests." - interviewee I (senior consultant)

Although the interviewees overall indicate similar perceptions and experiences, some individual differences can be seen from their answers. Firstly, some informants provided more extensive feedback on the subject matter than others. Some had reflected more deeply on the issue prior to the interviews and came more prepared. It is evident from the responses that certain interviewees relate closer than others to this research question and field of study in their professional field and everyday work.

For example, interviewee I, a senior consultant working with user adaptation of M365, had studied similar research fields as this thesis, enabling them to reflect on this practical case in a broader and more theoretical context. Even though they personally had a positive user experience of 2FA, they believed it not to be perfect, and speculated that this might be caused by lack of user perspectives and involvement from the developers of 2FA solutions. Later, they expressed a thought that the principles of usable security might revolutionize future IT security products. Others appeared to be prompted by the questions to articulate their experience for the first time ever. For example, interviewee C worked with technical sales, and had not previously given much thought to the user experience of 2FA. They had always used the SMS solution, because it had *"always worked fine"*. In fact, they had no knowledge of the Microsoft Authenticator App, and acknowledged that it was simply not in their personal interest to seek other solutions than SMS.

"I don't remember. I think I have just always received an SMS from Microsoft. So that's really just what I can relate to. I don't remember how I did it back then. [...]. So, I don't know that [the Microsoft Authenticator app] exists, quite simply. I'm not curious enough." - interviewee C (solution advisor)

Secondly, their professional roles, and consequently their work tasks, affected the practical application of 2FA in their workday. This includes how many times a day they are asked to authenticate, for what applications, and in what situations. A few informants reported that they only needed to authenticate one or zero times a day, without thinking that it was too frequently. Interviewee I on the other hand, was one of the interviewees that had to use 2FA more frequently than others. As mentioned, this informant worked with the implementation and user adaptation of Microsoft-tools of Atea's customers, and therefore had a Microsoft-user for each of their customers' Microsoft-environments. This meant that the informant had a list of their different users in their Microsoft Authenticator App, and on days with a lot of work with customers, the informant felt they had to authenticate at short intervals. Both interviewee I and H, who both worked in End-User Computing, had a similar experience regarding customer meetings. They felt that requests to authenticate successively appeared before customer presentations, making the customers wait while they themselves felt stressed and unprofessional.

Another individual difference was brought up by interviewee H; consultants are supposed to report their hours in the digital timesheet every single day, but in reality, it is much more common to do it once a week. To log into the digital timesheet system, one needs to use Microsoft two-factor authentication. Meaning that for those consultants who actually log their hours daily, it adds one additional authentication process for each day.

4.2.1.2 User Experience of Microsoft's Two-Factor Authentication Solutions

Most of the interviewees preferred the Microsoft Authenticator App over other Microsoft 2FA solutions, like SMS and phone call, but also over the Entrust-app and other solutions they used privately. The app is also what is primarily recommended in Atea's internal policy.

"Yes, [the Microsoft Authenticator App] is gold. I'll be surprised if anyone says something else." - interviewee B (account manager)

Even though the interviewees generally preferred the app, it was not because they experienced other solutions as significantly worse. The discrepancy in user satisfaction was often just marginal, but enough to make a difference. The interviewees described the Microsoft Authenticator App as less cumbersome than the other apps and some saying it has a seamless integration with M365-applications.

"[The Microsoft Authenticator app] is the easiest to operate. But I wouldn't say that the Entrust app is difficult either, but [the Microsoft Authenticator App] is a few seconds faster." - interviewee A (regional manager)

"I can't think of [a 2FA-provider] that works better than Microsoft, really." - interviewee F (solution advisor)

The interviewees occasionally experienced that the app did not function as intended, i.e. they experienced technical issues. This would result in the user having to restart the authentication process in the app, or select an alternative method of authentication, e.g. receiving an SMS.

Several informants commented on the difference in the practicality of the 2FA-process, depending on the devices utilized in the authentication process. If the authentication occurs on a login on the mobile phone, using SMS is easier because then you can simply click on the link received in the SMS. Interviewee D described this as a more seamless experience. While, if you are authenticating on a computer, using SMS requires the user to log into their phone as well. Interviewee H preferred SMS over the app when authenticating on the computer, because of the possibility of receiving the SMS on the smart watch while seated in front of the computer, removing the extra steps with using the phone.

"I actually prefer the SMS-version because then I get the message on my smart-watch, and then when I'm sitting by my computer, I can see that "yes, enter the code", instead of having to physically pick up my phone, use face ID and then enter a number." - interviewee H (consultant)

Several interviewees expressed their preference for biometric factors in the authentication process, i.e. fingerprint or facial recognition, because they experienced it as more effortless.

"I think it's nice when you can use biometric factors. But when you have to use SMS, open the SMS, enter the code - then I think it's too cumbersome. But that is a bit like a first world problem. It takes 3 seconds." - interviewee B (account manager)

Not all of the interviewees had experienced the new number matching feature within the Microsoft Authenticator App at the time of the interviews. However, those who had, acknowledged the additional step it requires in the authentication process, but at the same time the enhanced security it provides. Evaluating the entire authentication process, including the number matching feature, compared to the previous version, the opinions among the interviewees ranged from those finding it slightly more cumbersome, to those experiencing it in the same manner.

"[Number matching] worked, but the difference is maybe an extra click. So as an experience, I don't think it amounts to anything, neither positive nor negative." - interviewee F (solution advisor)

"I understand that it's a little more secure now. I actually have to type in something, instead of just having the phone look at my face and then I'm logged in. It's a bit more cumbersome, but then again, I understand that it's much more secure." - interviewee E (senior security architect)

4.2.1.3 Customers' User Experience of Two-Factor Authentication

The scope of our project and our selection of participants for both the survey and the interviews were employees at Atea. Nevertheless, we decided to include a question in the interviews to concern customers' experience of 2FA. While not all interviewees had enough experience to give us valuable information, a few provided some important insights.

Interviewee B was one of these, as they worked as an account manager in sales and sold the entirety of Atea's portfolio, thereby specializing in customer relations. Interviewee B highlighted that though customers are concerned with cybersecurity, economic priorities can often limit what security measures they choose to implement. Implementation of 2FA is not in itself particularly expensive, but smaller companies, and especially municipalities that have a tighter economy, have a higher bar to invest in 2FA.

However, it was observed by interviewee E, who had been in Atea for nine years, that there had been a positive development in the last few years in customers' approach to 2FA. They believed that implementing 2FA for customers today was an easier process, as customers no longer refer to excuses like 2FA time consumption, or using private devices for work-related tasks. Interviewee E believed this to have a correlation with the cybersecurity culture at the customers, which is discussed in section 4.2.3.5.

4.2.2 Challenges using Two-Factor Authentication

4.2.2.1 Frequency of Two-Factor Authentication Requests

A challenge encountered by some employees was the frequency of authentication requests. Several informants reported that they need to authenticate far more frequently when working from home, than from the Atea office network, as verified users. This is especially true if one does not log on to Atea's VPN first thing when working from home. Interviewee B explained that they felt frustrated by the frequent need to authenticate on various devices while working from home.

"If you're working from home, it's quickly two to four times, because you have to authenticate for the VPN if you're going to access something special there, like you're logging in to Microsoft 365 and the digital timesheet, and then there may be [a request to authenticate], in case you're logging in to some customer's application." - interviewee H (consultant)

Interviewee C expressed a similar viewpoint, noting the redundancy of having to use two-factor authentication while on the secure and verified Atea network in the office. This is experienced by the informants as unnecessary 2FA, as elaborated on in the next section.

The frequency may also differ depending on what device one is using when needing to authenticate. Several interviewees pointed out that authentication requests occasionally happen more frequently when authenticating from the mobile phone. Interviewee G, working as a business manager, was one of the employees using Mac instead of a Windows computer, and noted how Mac-users will be prompted to authenticate several times when opening the Windows desktop, which they expressed caused slight irritation.

The interviewees did not believe the frequency of 2FA requests to be a substantial challenge, even if they sometimes felt they needed to authenticate too frequently. They argued that this is because of the limited time it requires, and the security benefits they know it provides.

4.2.2.2 Illogical Authentication Requests

When asked if there are any situations in which they believe 2FA is illogical, a few situations were mentioned by the interviewees.

Several informants experienced minor frustration on excessive use of 2FA while at the Atea office network. As they are already connected to the secure network, using a secure and authorized computer, on a limited physical space, they therefore felt the authentication to be unnecessary and illogical. Interviewee A exemplified this with how they need to use 2FA to log into their internal digital timesheet management system. This application does not contain critical business information. Another interviewee used the word "hopeless" to describe their feelings toward this situation.

"We have an internal application where I need to use 2FA everyday, even when I am at my desk. Every time I open that application I need to authenticate, which I don't understand. I have already proved who I am by using my Atea computer and using the Atea network. I really don't understand why I have to use 2FA in this situation." - interviewee A (regional manager)

A few informants experienced the authentication requests as excessive when opening several applications simultaneously, especially from the same provider, like several Microsoft applications. In this case, informants felt it should only be necessary to do it once when opening the first application. As also mentioned in the survey results, interviewee E explained that the frequency of 2FA could have been less if the SSO had worked better and faster across applications. They felt this should especially be expected across Microsoft applications. Still, they justified this negative experience, explaining that if they had been better at closing all their applications properly, the SSO would have worked more as intended.

"When I have authenticated myself one time in a Microsoft app, one would think that I would get authenticated at the second in the other Microsoft apps, but I don't." - interviewee E (senior security architect)

4.2.2.3 Errors During the Authentication Process

Despite all interviewees having an overall satisfiable user experience of 2FA, and being successful in using the technology, they still experience a few different errors.

Both systematic and human errors were discussed as challenges. Some expressed that the Microsoft Authenticator App occasionally stopped working, due to some systematic error, including the app freezing. When using 2FA on the phone to log into other applications on the phone, interviewee F found it inconvenient because they first had to open the Microsoft Authenticator App and authenticate, and then approve the 2FA-request, and finally waiting for the authenticator app to jump back to the original app that requested 2FA (e.g. Teams). If something happens in this process, interviewee F noted how one has to do the whole process once more, except the next time using an alternative method of 2FA.

"So there are some challenges with [the Microsoft Authenticator App]. I just don't understand why this couldn't be done in a better way." - interviewee I (senior consultant)

Interviewee C expressed appreciation for the SMS-version, but had discovered some sort of malfunction on their phone. When receiving the SMS, they go back to the app that requested 2FA, e.g. Teams, and try pasting in the code from the SMS. The interviewee mentioned this as a smart feature because one does not have to write the digits manually, except that this feature did not work on their phone, making it more cumbersome. This worked for interviewee D, saying that it worked well on the phone where the code is applied automatically. Yet, it is more troublesome when the authentication request is on the computer, since the code here *has* to be typed in manually.

When discussing errors in the app, interviewee D highlighted how also human errors, i.e. errors caused by users, should be handled and resolved with equal importance as technical errors. Human errors may appear minor and simple errors to fix (in comparison to technical errors), such as incorrect app settings, but when users are never made aware, they are never able to correct the issues, and it may still have significant consequences, like them not being able to use the app. Interviewee D explained how users tend to take the most convenient and low-effort way around an issue in the moment, even when knowing that investing a little effort initially could lead to long-term benefits.

"The typical user; we only do what is needed to get things to work, always the easiest way." - interviewee D (solution advisor)

Three informants (interviewee C, D and G) did not use the Microsoft Authenticator App as their primary method for authentication, but rather SMS. The reason behind the interviewees' decision not to adopt the app was primarily due to their inability to effectively configure the app. Nonetheless, they acknowledged that the app is recognized as the standard procedure for authentication at Atea. Interviewee D used SMS for 2FA because they had not enabled the app to operate correctly. This informant was not satisfied with their choice of 2FA because they knew SMS is not the most secure option. The interviewee had not bothered asking colleagues in Atea for help with this issue, since SMS had always worked. The only way they would have fixed the app and used it would be if the SMS-version was deactivated or disabled.

"I use SMS, and I think that's not that good, actually. Because it's not the most secure, you're actually supposed to use the app, but I haven't gotten the app to work. [...]. I think that maybe, if it had worked, I would have preferred the app." - interviewee D (solution advisor)

4.2.2.3.1 Entrust

When using the Entrust app for internal systems of Atea, several informants reported technical errors, expressing that it is not as stable as the Microsoft Authenticator App. According to interviewee H, Entrust *"screws up a lot"*. Sometimes, during remote work, they have to restart the authentication process ten times, which results in postponing the task at hand. Interviewee C demonstrated how the Entrust app is used, and when an error happens, this creates a common frustration as the user is not informed as to why it happened, or if they can immediately try again.

"When I am asked to approve the authentication request [in Entrust] I think there are too many steps before I can finally push "OK". Sometimes it just disappears and leaves me waiting, wondering what happened. Occasionally it doesn't work and I'm like "Do I have to wait until tomorrow?"" - interviewee C (solution advisor)

4.2.2.4 Suggested Solutions to More Seamless Two-Factor Authentication

When asked, most of the interviewees did not have any specific suggestions, or were able to imagine a more seamless way to do 2FA than how it is done today. This could be because they were sufficiently content with the current solutions, or because they did not have the knowledge about other solutions than what they were currently using in Atea or otherwise. Interviewee D interestingly expressed a viewpoint that security measures are not *supposed* to be easy.

"There are no security measures that simplify anything. And that is not their function either." - interviewee D (solution advisor)

On the other hand, a few interviewees did recognize that 2FA is no longer considered as secure as it once was.

"And we no longer know how secure 2FA is. Only a year ago, it was recommended for everyone to have. Now we don't know if it's enough." - interviewee B (account manager)

One specific technology that was mentioned by both interviewee E and I, was Windows Hello. Windows Hello is the name of Microsoft's biometric security system, where the biometric technology is built into the computer. This means that users do not need to use their phone when authenticating on their computer. Interviewee E felt this would be easier as there would be a more seamless authentication process, without any pop-ups. The interviewee also addressed how Windows Hello is more secure than their current 2FA solution, as the machine itself is verified from the producer. With the computer as a factor itself, one avoids the risk of MFA, i.e. when some attacker's proxy is able to decode and read the authentication code. Interviewee E compared Windows Hello to how you log into your mobile phone using facial recognition, and then simultaneously are authenticated to use all your applications. Also, interviewee H expressed, without particularly mentioning Windows Hello, how facial recognition on the computer as a factor would be easier than needing to pick up your phone for authentication.

4.2.3 Cybersecurity Awareness and Culture

Generally speaking, all of the nine interviewees described the internal cybersecurity culture at Atea in a positive and satisfactory way. They reported that both the cybersecurity culture and cybersecurity awareness are strong. IT security is incorporated to different degrees and in different ways throughout the entire organization. It is therefore crucial to ensure that every employee is involved in IT security and understands their responsibility toward it. When asked, all nine interviewees said they work with IT security in some capacity. As a consultancy firm, and as such a large European enterprise, IT security is a crucial part of what Atea do. This necessitates the promotion, discussion and assurance of IT security, not only within the organization, but also for their customers and partners.

"It's the most important part of our job, to secure the values of the businesses we work with. So that's clearly a focus we have. [...] Security permeates all processes here." - interviewee B (account manager)

Several interviewees emphasized that working in a large and reputable IT enterprise such as Atea engenders certain expectations regarding the internal IT security. Further, this may result in one taking IT security for granted. For instance, interviewee I explained that since their computer is enrolled in the Atea domain, they assume that security breaches simply would not happen, as long as they use the computer for work-related things. This is because the correct measurements are already ensured on the computer. The interviewees attributed this responsibility to various elements like the structure of the organization, the internal software and hardware in use, and the proficiency of the in-house security department.

"I'm perhaps not so aware of [IT security] in everyday life. It's more like, I feel confident that the programs and frameworks we use are taken care of from a higher level of IT security in Atea." - interviewee G (business manager)

4.2.3.1 Knowledge Sharing

One aspect of the cybersecurity culture several of the interviewees highlighted, was the open and collective discourse about the topic that occurs on a daily basis. Being a member of a team that prioritizes sharing of both explicit and tacit knowledge is essential. This is an important factor that contributes to creating awareness for all employees and further maintaining a good security culture. Discussions take place both casually among colleagues, as well as during different types of team- and staff meetings, where management also addresses the issue. Moreover, this conversation extends to dialogues with customers. The interviewees described this transparency concerning IT security as focusing, underlining the significance of IT security and making it a focal point throughout the organization.

"Enormous - we don't talk about anything other than security on a daily basis, we don't. So there is a big focus. And I can see both in myself and in colleagues that we are becoming increasingly aware of potential threats. So when we receive an email from someone we don't know, there is a full discussion; what is this? Can we trust it? So the focus is definitely there, that's for sure." - interviewee F (solution advisor)

Knowledge and competencies among the employees were another element the interviewees claimed to contribute to the good cybersecurity culture. The employees asserted that the understanding of IT security is a central factor in their acceptance and appreciation for the implementation of two-factor authentication in the organization. While most interviewees shared this perception, it varied to what degree the informants displayed this knowledge in the interviews. Those who did not particularly work within the IT security field themselves, emphasized how being surrounded by colleagues with such expertise, raises and improves awareness. Interviewee E highlighted how IT security has been a significant strategic priority area the last ten years in Atea, increasing from 10 to 170 employees exclusively working with IT security both internally and externally, and continues to be so. Interviewee I explained how the in-house expertise functions as a type of ambassador for cybersecurity, in a way, raising its status within the organization.

"Yes, as I said previously, we have very good security competencies here [in the Trondheim office] and generally in Atea. So I think that IRT [the Incident Response Team] are kind of like rock stars. I think it's cool that we have very high competencies in this area." - interviewee I (senior consultant)

In Atea, knowledge and awareness are distributed and taught through a variety of means. Apart from internal training, different disciplinary teams meet up on a weekly or monthly basis to discuss topics such as IT security. For instance, interviewee H, a consultant specializing in M365-products, participated in a disciplinary team that met biweekly to receive updates on the latest developments in cybersecurity and Microsoft. Interviewee H also mentioned that Atea hosts its own podcast, which releases a new episode every week on streaming platforms, that frequently features discussions on news related to IT security. In the past, interviewee H recalled, the security department in Atea distributed an internal newsletter to the entire organization with the latest IT security updates, with practical tips, e.g. "what to look out for". Even though it would vary how interesting and relevant the content in the newsletter was, interviewee H was under the impression that most of their colleagues read it, and that the newsletter therefore increased awareness and highlighted IT security.

Still, the interviewees acknowledged that the level of cybersecurity expertise likely varies among departments and teams. However, they did not assert this with certainty, as most interviewees did not have formal experience from other than their own team. The interviewees did not seem to believe that though the knowledge between teams varied, the culture for cybersecurity was better or worse throughout the organization. Talking about the cybersecurity culture, the interviewees seemed to regard Atea as a whole, more than as isolated units. Specifically about the knowledge and culture of two-factor authentication, interviewee F believed it not to vary as much, not in the same way as the expertise otherwise varies between teams.

4.2.3.2 Training in Two-Factor Authentication

In many respects, Atea places a significant emphasis on the training of their employees. Yet, in regard to the use of 2FA as a security mechanism, there is very limited training, neither on its purpose or practical application. In a later interview, it was revealed that there is in fact a module in Motimate that contains some information on 2FA. This particular interviewee had knowledge about this course due to their authorship of the course. However, the large majority of the other interviewees did not mention this course, and they did not consider the lack of training in 2FA as a disadvantage. They reasoned this mostly because they felt their existing knowledge was sufficient to use the app and they understand the necessity of 2FA in their everyday work.

"I must admit I don't think I've had any training. [...]. But at the same time, perhaps I haven't quite seen the need for it either in my everyday work with the applications I use, because it has always worked." - interviewee A (regional manager)

"I managed fine without training, and I also understand why we use [2FA]." - interviewee C (solution advisor)

Interviewee I, on the other hand, had a different perspective on training. A lot of this interviewee's work as a consultant with customers consisted of user adaptation of M365. In this work, they stated that it was considered of utmost importance to include the training of security competencies, like why and how to use the tools in M365 in a secure way. This reflected in their perspective on internal training at Atea. They felt like a great amount of the training they got was with first and foremost the customers in mind, but not so much on the consultants as employees and users of these digital collaboration tools themselves. Interviewee H had a similar experience from working with user adaptation as interviewee I, and to some extent shared their view. Though they had not experienced difficulties as a result of no training in 2FA, they acknowledged the value of it.

"I work with training myself, so I think that's really, really unfortunate. Especially in an IT company like ours - we're really good at IT security when it comes to our customers, so we should be equally good at internal training." - interviewee I (senior consultant)

Interviewee I was also the only interviewee that recalled the 2FA training in Motimate, but did not believe it to be sufficient. They highlighted how it was a short five-minute course they had taken many years ago, and that a lot has happened in the cybersecurity threat landscape since then. When asked, a few of the other interviewees reasoned that it was likely that some training in 2FA existed or was perhaps even something they had completed.

"I can't remember ever really being part of a training [...]. Maybe there's something in -, we have this internal training portal in Motimate, maybe there's a course I went through a long time ago, but -. No, if there has been any training, it perhaps didn't make much of an impression on me since I can't remember it." - interviewee F (solution advisor)

4.2.3.3 Motivations for using Two-Factor Authentication

The most reported motivation for using 2FA, was the understanding and awareness of the cybersecurity it provides. The risks in the current threat landscape and the possible repercussions of a security breach, were mentioned by several informants. The significance of MFA for cybersecurity, i.e. to protect data assets, is also what is communicated internally as the main motivation. The informants felt that the security advantages 2FA provides, outweighs any inconvenience it may pose in practicality.

“I understand why I should [use 2FA], and I think it's important that we do it too. So for me, it's not about the pros and cons [of the practical implementation]. It's a necessary evil.” - interviewee D (solution advisor)

Interviewee A had experience with the new number matching feature in the Microsoft Authenticator App, and upheld that the added security is more motivating than the extra effort it requires.

“No, it was simpler before, now there is an extra step. But it’s simple; if it helps us maintain security, I can press those two numbers, it will be fine. The downside is much greater if we behave unsafely. A little effort to ensure security is worth it.” - interviewee A (regional manager)

Knowledge and understanding were also a point where the interviewees noted a difference from some of their customers. The consultants observed that customers who experienced difficulty in recognizing the significance of implementing 2FA within their organization, frequently failed to perceive the security advantages as a compelling motivation.

"And perhaps that's where the challenge comes for those who don't understand it. Now, I don't think there are such huge challenges at Atea, but if you were to go to a municipality and talk to people who work there but don't work in IT, you would probably get a different answer and not understand why.” - interviewee E (senior security architect)

Some informants highlighted the importance of feeling personally secure through protecting their identities. Interviewee E explained how there has been a shift in this perspective over the last years, whereby the discussion has evolved from protecting company data to first and foremost protecting users' identities and privacy. This has made users more skeptical, more aware and ultimately more motivated to utilize measures such as 2FA.

“Yes, I want to protect myself. Myself and my values, then, should know that it is securely stored, and that no unauthorized person should get hold of the private information.” - interviewee A (regional manager)

For informants who work closely with customers, like interviewee B as an account manager, the responsibility for the customers seemed to emerge as a motivation for using 2FA as a security mechanism. In the survey, the only written answer to the question about motivation was also about this responsibility for the customer. The respondent highlighted their role as an administrator of customer systems and the worst potential risk of bankruptcy for the customer in the event of a security breach.

“But I’m the one who is responsible for the customer getting what they asked for. And then one can’t be secure enough.” - interviewee B (account manager)

When asked specifically what their motivation for using 2FA is, a considerable number of respondents’ first response was because it is simply mandatory in the organization, as per company policy. In other words; the use of 2FA is a prerequisite for employees to gain access to systems and perform their job functions. Interviewee C actually put their motivation in that order when asked, answering: *“Number one; we have to. Number two; it is security”*. Later, Interviewee C also argued that 2FA being imposed in Atea in itself provides a feeling of security.

"I also feel more secure when 2FA is required. I feel safer then, and when I'm at work using email and Teams, I can see that I feel a little more secure - it gives me a sense of security.

That's why I think it's okay to use it. Well, there aren't really any other motivations." - interviewee C (solution advisor)

Interviewee D argued that 2FA being imposed means someone qualified has made this decision for the users' best, expressing that they trust their evaluation.

"Yes, I think that there are some people who know more than me about this and have decided that it should be this way, and then I choose to trust that. Simply because you can't involve yourself in absolutely everything." - interviewee D (solution advisor)

This argument from interviewee D, leads to another way some interviewees deemed their motivation, i.e. they do not have a particular or strong sense of motivation. As interviewee D stated, they saw no gain in involving themselves or having an opinion in decisions about 2FA or other matters in which they had no expertise.

"I only adhere to what the company has laid out for us, on applications where 2FA is required." - interviewee A (regional manager)

4.2.3.4 Qualities of Employees

There are several qualities of employees that contribute to a good security culture at work. The interviewees mentioned some important qualities that we will now present.

Almost all informants drew attention to competency and knowledge, as mentioned, as being important qualities of employees. Specifically, there is an emphasis on understanding the various threats that exist, the role of cybersecurity, the necessity of 2FA, and the potential consequences of unexpected events. It is also fundamental for employees to have a genuine desire to protect oneself. Knowledge is the key to comprehending the importance of a layered approach to better security. Despite the expectation for employees to acquire knowledge, interviewee F pointed out the importance of humility, i.e. acknowledging the limitations of one's knowledge. Employees that do not understand cybersecurity and do not pursue gaining knowledge, will have several challenges with 2FA, resulting in a negative user experience. Most employees stated that they have a positive user experience of 2FA and some stated that they have a neutral user experience of 2FA. They meant that this UX was rooted in the competencies they have acquired due to the good security culture.

"I think that the resistance against two-factor authentication is rooted in ignorance. People don't know the consequences of not using it. I think that's how simple it is. If people knew the threats from our [IT company] point of view, I can't believe anyone would be negative about using it." - interviewee A (regional manager)

Being curious and asking each other questions were emphasized by most interviewees to be important personal qualities. This includes having open discussions about cybersecurity and 2FA with colleagues. Examples of such questions include inquiring about new security features and expressing doubts about suspicious emails. It was highlighted by a couple of the interviewees how every employee of Atea should strive to align with the core values of the organization. One of these values is curiosity, i.e. being curious about the environment, situations, employees' knowledge, emails that appear to be fake and so on. Another core value is 100% responsibility at all times, relating to both security and other aspects of the company.

Several interviewees also noted that one should also be skeptical. They exemplified this as looking twice at emails or text messages one receives, making sure they are legit. According to interviewee E, Norwegians are among the most naive people in the world, meaning that being skeptical is not in our nature, which is why one should be aware of what we trust. They also mentioned that openness about these issues, like people sharing stories about having their identity stolen, sharpens awareness, skepticism and curiosity. This again leads to understanding how one for example should approach an email asking for personal information. Interviewee I argued that skepticism toward specific situations should not be endured alone, but openly discussed, by setting a low threshold for both seeking and providing help.

A few informants mentioned attentiveness as an essential quality of employees. Interviewee A stated the ability to assess threats and having a conscious relationship with where you leave your own information, as significant. Maintaining a high level of situational awareness, i.e. having security in the back of your mind at all times, is crucial in maintaining a good security culture. Interviewee D expressed how training can provide more attentiveness and consciousness to the security aspect and how easily security breaches can happen.

"We should have some training in discovering how easily fooled we are, because I think we are. I think everyone is easily fooled; I think everyone is overestimating their own abilities. It's proven many times: people in general are overestimating their own ability in knowing stuff. For some reason we want to be proud." - interviewee D (solution advisor)

Interviewee H pointed out the observation that younger generations tend to have a more inherent understanding of cybersecurity, and therefore also its importance. This contributes to the development of a good security culture. Young people following the current discourse and development in these topics, are more aware of the numerous security breaches happening, which can motivate them in acquiring knowledge to prevent future attacks. The informant also highlights how older users will have a more difficult time because technology is often not as intuitive to them. According to interviewee D, it is still noteworthy that it is often those who believe they have the best control, that are more susceptible to cyber attacks.

"I have read that those who think they have 2FA under control are those who have the greatest chance of being a target of a computer attack." - interviewee D (solution advisor)

Two interviewees drew attention to the importance of including the customers as part of the company's security culture. They emphasized that prioritizing the customer's success is crucial, as they as a consultancy firm do not want any negative incidents to occur for their customers. Atea's business model regard selling knowledge and competencies to their customers. Atea could therefore indirectly enhance their customers' security culture by first ensuring they maintain a strong security culture internally.

4.2.3.5 Customers' Cybersecurity Culture

The interviewees that worked closer with customers, and had formed an opinion about their cybersecurity culture, had some mixed views. Firstly, they felt customers were overall concerned with IT security. Moreover, the consultants felt that this was primarily driven by a fear of the potential consequences of a security breach. This impression of the customers was formed by the current discourse on these topics, including what is presented in the media. At the same time, the interviewees recognized that their customers often lacked competencies and expertise, particularly in comparison to Atea. It should be noted that these observations did vary between customers and customer-segments, and that individual differences exist.

"The clients are very concerned with [IT-security]. It's a repeating topic in all customer dialogue. Security is the most important thing for them. [...] There's a lot of horror stories in the media. [...]. They are terrified of [the consequences]." - interviewee B (account manager)

Interviewee B also underlined the importance of communicating to the management of the customers that security and the use of 2FA is their responsibility. If the responsibility of security in a customer company nevertheless lies on Atea, the relationship between Atea and the customer would weaken if the customer experiences a security breach. Another observation by interviewee B was the issue among customers in that the IT-department is often not given sufficient resources to implement all security measures they wish to, yet fear they will get the blame if a security breach actually occurs.

Several informants believed that Atea, to some extent, had a greater culture for cybersecurity than many of their customers. Interviewee E suggested that customers' security culture might be weak because employees are not well enough informed as to why 2FA is essential for ensuring IT security. Making customers understand what 2FA is and how to use it, one has a greater chance at successful implementation.

4.2.3.6 Consequences of an Unsatisfactory Cybersecurity Culture

When asking the interviewees what some consequences of their alternative solutions are, or "workarounds" as employees referred to, numerous points were mentioned. Some have a more negative outcome than others, but all of them are to some degree a consequence of an unsatisfactory cybersecurity culture.

Firstly, the negative user experience of 2FA may result in employees postponing tasks, due to sometimes cumbersome login situations. Several interviewees explained that if they work from home and countless authentication requests start appearing when they turn on their computer, they will occasionally postpone the task they meant to do for when they return to the office. Interviewee E pointed out that for many systems there are no ways around using 2FA, so if they do not want to authenticate themselves many times, they have to defer what they had planned. This challenge can contribute to several employees creating a culture for postponing tasks.

A more severe consequence is regarding security breaches and malicious attacks. This is a common fear for Atea's customers, as interviewee B mentioned; municipalities are terrified of being hacked, while this is also a genuine risk for Atea. Interviewee C elaborated on a test that was done internally at Atea to create awareness around how easy targets all users are. The test entailed an email that was sent out to the whole organization, to discover whether or not the employees would perceive it as a scam. Maybe this could minimize the risk of employees opening links from an unknown source in the future. Many employees clicked on the link because it seemed to be from a colleague in Oslo. A colleague of interviewee C was one of them. Another email was then sent out an hour later stating that the first email was an attempt of an attack. The employee panicked at the time, but luckily it was only a test. It has been mentioned by several other interviewees that more of these types of tests should be done, because people should be aware of their own vulnerability as a target. Interviewee E here highlights the importance of training to prevent disasters from happening, because a great deal of the mistakes occur due to ignorance.

"If employees don't know how to use a system, things are easily done wrong." - interviewee H (consultant)

Ignorance is only one example that can lead to the worst consequence, which is having your identity stolen. This can mean personal loss (e.g. economic), emphasized by several informants. Companies can also experience bankruptcy. Fortunately, these situations rarely happen.

4.3 Summary of Quantitative and Qualitative Analysis

After analyzing both the survey and the interviews, we have compared the results. We have omitted some results deemed not as important. As the survey consisted mainly of answer options, the interviews contributed with much more breadth and depth to the research. Yet, the results will be compared to see how the user experience of 2FA differs or is similar between respondents. It is also worth noting that the survey generated 122 answers, while only nine interviews were conducted. Some questions have also varied between survey and interviews, due to convenience. Only interviewees had the opportunity to explain themselves further, answer outside the scope of the questions, answer follow-up questions etc.

4.3.1 User Experience of Two-Factor Authentication

All respondents expressed that the app is easy to use and are overall satisfied with this method for 2FA at work. It is nevertheless not perfect, in the words of an interviewee. Most employees agree that the Microsoft Authenticator App is the best option for 2FA, among the alternatives they have tested. During interviews, some participants have expressed a preference for using SMS as a means of authentication when accessing their accounts via phone. They cite the convenience of SMS codes being automatically applied to the login process on their phone, eliminating the need to open the app for authentication. Conversely, when logging in from a computer, employees are required to pick up their phone as a second factor of authentication. Almost all employees stated that the app increases the feeling of security in the workplace. It should be noted that utilizing the same device for login and as the second factor of authentication is slightly less secure than using two separate devices.

As stated in the interviews, the amount of times per day that employees need to use 2FA varies whether they are at Atea or working from home. We were not aware of this distinction prior to the survey and did therefore not distinguish between 2FA at different locations in the survey. The average times interviewees use 2FA per day varied, but were usually in the range of 0-4 times per day, i.e. up to four times at the home office, and down to zero times at Atea. In the survey, 66.4% of respondents use 2FA 2-7 times a day on average, i.e. 37.7% answered 2-3 times and 28.7% answered 4-7 times a day. Around half of the employees feel that authentication requests happen too frequently, but the interviewees highlight that they know the security benefits and how that is enough to accept more authentication than one feels necessary. Whether or not this reason is enough for the respondents in the survey is difficult to tell, as they were never given an opportunity to explain. Sometimes, some employees think that 2FA hinders efficiency in the workplace.

When answering a survey with predefined multiple answer options, it is easy for respondents to tick off every answer they agree with. The most popular motivation for using 2FA from the survey seems to be the security benefit, i.e. 111 answers, but all interviewees mentioned the requirement from the company as the first motivation. Even when employees state that *the app* increases the feeling of security in the workplace (average score 4.11 out of 5 on a Likert scale), just half (58 out of 122) of the respondents answered as a motivation that *2FA* makes them *feel* more secure. Interviewees also mentioned knowledge and understanding as motivating factors as well as their responsibility for their customers.

4.3.2 Challenges using Two-Factor Authentication

One mentioned challenge concerns the frequency of authentication requests. Survey respondents feel they must authenticate too often, while this seems to be less of a challenge for the interviewees. Only nine interviewees were asked, and could be the reason for this distinction.

Some employees from the survey and a few from the interviews expressed how authentication requests often seem arbitrary and illogical and appear at inconvenient times, e.g. before a customer presentation, mentioned by one interviewee. It was also expressed by several employees how it is difficult in some situations to see why one must authenticate. This is especially true when on the safe network of Atea, but also everyday logging into a timesheet program that does not contain any sensitive information.

Sometimes employees have smaller issues or errors with the Microsoft Authenticator App, but overall it works as intended and they say that it occurs rarely. Some interviewees have never been able to get the app to function, meaning that they use other methods for 2FA, like SMS. Some of these are saying that they would have preferred the app if it worked. The Entrust app often malfunctions, according to many employees.

4.3.3 Cybersecurity Awareness and Culture

All employees expressed that Atea has a positive culture for IT security, yet there exist some concerns regarding potential security breaches. Some employees stated in the interviews that they know how naive people are, and that tests have been conducted that demonstrate how easily people are fooled. Many interviewees mentioned that employees might have expectations to Atea, as an IT company, to always ensure adequate cybersecurity. However, it is important for employees to remain aware of potential security risks and not solely rely on the company. While employees feel they receive satisfactory training in IT security, including in 2FA, several interviewees were unable to recall if they had actually received any training in 2FA. Despite this, one interviewee did highlight Atea's commendable competence in training customers and suggested that the same quality should be applied to internal training.

There are several reasons for this good security culture. During interviewees, a recurring theme was the culture for knowledge sharing and curiosity, the latter also being one of Atea’s core values. Different personal qualities that individuals hold were also discussed, and how the Atea employees share them. These qualities are for instance skepticism and attentiveness to cybersecurity threats. These are traits that incline people to acquire a better understanding of cybersecurity measures, like 2FA, which contributes to a better user experience.

Beside qualities of employees contributing to a good culture, there exist several questions only given to interviewees, meaning that answers cannot be compared to survey results. Number matching is one of these. This feature was implemented after the survey was done, but was still added to the interview guide, so that the interviews were updated on all new security features. We also included a question in the interviews concerning customers’ user experience of 2FA and consequences of a poor cybersecurity culture, but this was only to get an elaborate answer that would not be possible in the survey. In the interviews we also asked if the informants could think of a better solution to 2FA. Windows Hello was one solution mentioned.

5 Discussion

In this chapter we will discuss the empirical findings from the survey and the interviews in context with the theory presented in chapter 2 to shed light on the research questions. Maintaining the structure of the research questions, this chapter first discusses the general user experience of 2FA, then identifies the three main challenges, and finally, it provides a comprehensive analysis of the cybersecurity culture and its impact on the user experience of 2FA.

5.1 User Experience of Two-Factor Authentication

Several authors have documented issues from a user's perspective concerning both human and technical aspects in regard to 2FA (Acemyan et al., 2018; Gunson et al., 2011b; Marky et al., 2022; Stanislav, 2015). In our research we have found some similar issues that negatively impact the user experience that we will discuss further in the next section concerning challenges. We will now proceed to discuss the more general user experiences documented in previous research in relation to our results.

Virtually everyone in the survey answered that they have an understanding of 2FA. Though the interviewees were not explicitly asked or tested about their knowledge of 2FA, their understanding was still confirmed during the conversations, in the way they discussed 2FA, though the level of expertise varied. For instance, the interviewees demonstrated a good understanding of factors, consistent with the definitions proposed by Gunson et al. (2011a) and Marky et al. (2022). Most interviewees also used their knowledge and understanding of the security benefits provided by 2FA, as noted by Dasgupta et al. (2017), as an argument to why they accept and appreciate the implementation of 2FA in the organization. This is different from what S. Das et al. (2018) argue, namely that users often have misconceptions or lack of knowledge about the security benefits of 2FA. However, our study examines an IT company, meaning that internal cybersecurity is not only a requirement to the organization, but an important part of the competencies and the culture among the employees. If we were to study another organization, the results might have been different. It was highlighted by several interviewees that Atea has been successful in teaching their employees about the security benefits of 2FA. If benefits are not evident for the user, the user will lack motivation to adopt the second factor.

The interviewees explained that they mostly preferred biometric factors, which is why push notifications with biometric approval is the most common authentication method at Atea. This aligns with a study by Abbot and Patil (2020) that found that push notifications were the most widely used and preferred method for 2FA. Text messages, physical hardware tokens and automated phone calls were ranked second, third, and fourth from the study, respectively. Some of the employees of Atea with more expertise in this area, expressed the benefits of using physical tokens, such as FIDO and Windows Hello.

The interviewees' competencies are not only seen in their understanding of the concept of MFA, but also in how to use 2FA and the technologies in a practical sense. This is supported by findings from a study by Colnago et al. (2018) at a university before and after the implementation of mandatory 2FA, which indicated that users found 2FA annoying, but not difficult to use. Our research found some similarities; the Microsoft Authenticator App scored an average 4.11/5 on ease of use on a Likert scale, but only 2.35/5 on annoyance and frustration. As Bevan (2009b) explains, experienced frustration is a relevant measure for both usability and UX. Further, continuous excitement is another measure Bevan suggests. Though the respondents did not display signs of excitement for 2FA as part of their work specifically, the interview respondents did show very positive feelings and engagement for cybersecurity and the cybersecurity culture in the organization, which naturally 2FA is a part of. Still, this is only two of several measures the author proposes, and can therefore not alone be used for a complete assessment of usability. Since we are researching user experience in a broader perspective, these measures and the responses gathered through our data collection, can in combination provide a sufficient assessment of the usability of 2FA.

Research shows that people tend to perceive 2FA as the most secure option for authentication (Gunson et al., 2011a), and SFA as the greatest for convenience and ease of use (Dutson et al., 2019; Gunson et al., 2011a). While we did not specifically inquire about this aspect during our survey or interviews, it became apparent that our participants recognized and valued the enhanced security that 2FA provides. Nevertheless, 41 respondents in the survey answered "I'm impatient" as a reason why they experience challenges, meaning that SFA would likely be more convenient for them. As a result, they seemed to be less preoccupied with its convenience as long as it did not significantly increase the time required for authentication.

Studies by Marky et al.'s (2022) have highlighted the importance of considering usability, trustworthiness, and required cognitive effort in tandem. According to their findings, these factors are interrelated and play a critical role in shaping users' experiences with a given technology. As such, a comprehensive assessment of a technology's effectiveness should take into account not only its usability but also the degree to which it is trusted, and the level of cognitive effort required to use it. When evaluating the usability of 2FA, we can turn to the definition proposed by Bevan (2009b). This definition considers how employees utilize 2FA as a means of authenticating and accessing systems with effectiveness, efficiency, and satisfaction. The responses generally paint a positive picture of the usability of the Microsoft Authenticator App. The respondents found that the app worked as intended to achieve its goal, in an adequate amount of time, and was easy to manage, i.e. low required cognitive effort. Simultaneously, the respondents displayed high levels of trust for 2FA as a security mechanism, mostly because they felt confident in their knowledge about the security benefits, and because they trust Atea's recommendation, given the nature of the company. This aligns with our expectation that researching an IT company would yield different results, given the paramount importance and significance of cybersecurity to both the company and its employees.

According to some studies, user characteristics correlate with the perception of 2FA usability, rather than the second-factor technologies used (De Cristofaro et al., 2014). This is not equal to what we found, but not contradicting either. During the interviews, it was brought to our attention by several participants that older users may experience difficulties understanding and using 2FA, resulting in suboptimal usability for this demographic. Though the age distribution in Atea is relatively young, and therefore does not represent a substantial challenge, it may differ from their customers, as also noted by the interviewees. We found no correlation from the survey that the older employees, thus few, found 2FA more difficult. Gunson et al. (2011a) conducted research on the usability of 2FA among different age groups and found that older users, in general, reported lower levels of usability compared to their younger counterparts. They are arguing that a lack of competencies is the reason. According to our research, the usability of 2FA is dependent on which second-factor technologies used, even more so than the results from De Cristofaro et al.'s (2014) study.

5.2 Challenges using Two-Factor Authentication

In the below paragraphs we discuss the three main challenges for the user experience of 2FA. These challenges have been considered significant due to their frequent mention and discussion by the informants. The challenges are compared to existing literature to answer the sub-research question "What are the challenges in two-factor authentication that users experience in Microsoft 365?".

5.2.1 Frequency of Authentication Requests

As mentioned in the correlation analysis (section 4.1.5), the more times employees must authenticate or the more time consuming they feel the app is, the more frustration they have toward the app. This is supported by De Cristofaro et al. (2014), who suggest that the frequency of 2FA is essential to how usable people perceive 2FA. Adoption rates of 2FA will, according to the authors, depend on the user experience. This research was done when using 2FA was voluntary. More frustration could potentially leave the users accepting requests without checking if the requests were logical, making the system less secure. In the case of Atea, using 2FA is company policy and employees cannot access systems if they deny using it. Nevertheless, we have reason to believe, based on the correlation analysis, that the user experience is still of importance to how well employees perceive 2FA. Marky et al. (2022) argue that it might be difficult for employees to afford the authentication process when they are required to do it multiple times. The management of a company should strive to avoid employees feeling frustrated in regard to the frequency of 2FA requests.

5.2.2 Illogical Authentication Requests

Authentication requests that were perceived as illogical and unnecessary were described as a challenge by several interviewees and informants. Abbott and Patil's (2020) research, which focused on a large US university, yielded similar findings. They discovered that user experience and acceptance of 2FA decreased when users were required to use 2FA for logging into university resources that did not contain sensitive information. During our research, employees of Atea expressed frustration when required to authenticate their identity while already on Atea's secure network or when logging into non-sensitive systems. Additionally, some interviewees experienced authentication pop-ups in non log-in situations, e.g. in the middle of a Teams meeting. These authentication requests are not only unnecessary, but they are also inexplicable, and represent a breach in the employees' established knowledge and understanding of 2FA. As mentioned by two respondents, unjustified frequent 2FA requests can lead to users approving fake requests. This is an interesting argument, as it links the practical dimension of authentication in everyday life, to more abstract psychological factors. As the authors' study focused on a university, it is reasonable to assume that employees of Atea, being an IT company, possess a greater understanding of the security benefits of 2FA and, consequently, have a higher level of acceptance toward it.

5.2.3 Errors During the Authentication Process

Technical issues will overall contribute to a poor user experience because the usability becomes unsatisfactory. Marky et al. (2022) argue that unsatisfactory usability could happen during the setup process of specific 2FA tokens or with a lack of integration with different operating systems. Some interviewees experienced problems during the setup with the Microsoft Authenticator App. It was also mentioned by one interviewee how the app had poorer integration with MacOS, than Microsoft Windows operating system, causing employees with Mac to authenticate more frequently. It was brought up in several interviews how the setup process of 2FA is perceived as less usable than the day-to-day use, which is supported by arguments from several authors (Acemyan et al., 2018; Ciolino et al., 2019; Reese et al., 2019; Reynolds et al., 2018). Acemyan et al. (2018) argue that a difficult setup process can discourage users from continuing the use of 2FA. We cannot say whether or not employees of Atea would stop using 2FA if the setup process was too difficult, because using 2FA is mandatory and most employees found the process to be satisfactory. Still, this highlights the importance of user support for those who experience difficulties. This may for instance determine whether they want to use the app or not.

5.2.4 Interrelations of the Main Challenges

The three challenges discussed above can be seen as highly connected, and should not be addressed isolated, but by recognizing their interdependencies. Firstly, the frequency of authentication requests is linked to the illogical authentication requests, as the more frequent the requests, the more likely users are to perceive some of them as unnecessary. This can be seen in how the informants experience the multiple authentication requests to different Microsoft applications; they are perceived as both too frequent and illogical. Secondly, technical errors can contribute to an increased frequency of authentication requests, as interviewees experienced failure using both the Entrust and the Microsoft Authenticator app, causing them to repeat the authentication. These challenges will overall affect the user experience, both individually and combined. Therefore, these challenges are interrelated, and addressing one challenge can potentially improve the other challenges as well.

5.3 Cybersecurity Awareness and Culture

Schein and Schein’s (2016) proposed three-level model describes an organization's culture, whereas the levels refer to different degrees to which a cultural phenomenon is visible to the participant or observer. Many of the elements in their model align with AlHogail and Mirza’s (2014) suggested definition of cybersecurity culture. With this definition in mind, Schein and Schein’s model can be used to describe the cybersecurity culture at Atea.

The first layer, the artifacts and creations, includes aspects that can be easily observed and interpreted by the employees, customers and the general public. The most prominent aspect of this layer discussed by interviewees, was the habits and internal routines regarding security in Atea. For the most part, interviewees brought up habits and behaviors that could be seen to contribute positively to the cybersecurity culture, but instances of this with a negative impact were also mentioned. The interviewees pointed out that knowledge and awareness sharing in both formal and informal settings played a crucial role in strengthening the cybersecurity culture at Atea. Informal settings contain the open dialogue that happens continuously in the Atea offices among colleagues. Formal settings include different types of meetings, training and disciplinary teams. The components of the first layer may be a factor contributing to the results of the survey, which found that Atea employees feel they receive adequate training in IT security and are not concerned about the level of competence their colleagues possess in this area. Further, the language and wording used by the interviewees when discussing matters of cybersecurity, leaves the impression of a professional, competent and positive culture.

Another element of the first layer is Atea’s explicit strategic commitment to the development of their in-house cybersecurity expertise. This is a continuously growing field in Atea both in terms of the number of people working specifically with it as experts, and how it is broadly implemented in the employee training. As interviewee I describe, they regard the Incident Response Team as “rock stars" of the organization. This view indicates the status the cybersecurity experts hold within the organization, which is possible not only because of their actual knowledge and competencies, but also because the other employees are able to acknowledge and understand the importance and significance of their work. A third element can be seen through the expectations for cybersecurity the interviewees had to Atea, which includes qualities in the physical devices, the software and tools in use, and the policies implemented. This way, the implementation of the Microsoft Authenticator App as the primary method for 2FA is in itself a prominent manifestation of their cybersecurity culture. However, the average response of survey participants stated that they were slightly above neutral concerned with security breaches at work. It is difficult to say if this is caused by internal or external factors, or human, organizational or technical factors.

The second layer to Schein and Schein’s (2016) model, values and beliefs, are explained by Parsons et al. (2010) as direction and guidelines that are supposed to guide employees toward a certain behavior. The core values of Atea, as brought up by interviewee G, are a prime example of this. These could also be seen as part of the first layer, since they are in fact a published list of values, yet how the values are in reality espoused to reflect individual assumptions is even closer to the core of organizational culture, and therefore discussed here.

Interviewee G especially highlighted the curiosity- and responsibility-values as highly relevant to cybersecurity. During the recruitment process, there is a strong emphasis on ensuring that candidates align with these values and continue to uphold them in their employment and work. Although the other interviewees did not explicitly mention Atea’s values in the same way as interviewee G, possibly because interviewee G holds a more explicit commitment to them as a business manager, curiosity, in forms of knowledge seeking and -sharing, was commonly identified as a key quality. These are both qualities that contribute to a good cybersecurity culture. Other commonly mentioned qualities were skepticism and attentiveness, which could be interpreted as a way of holding oneself responsible.

Other types of guidelines can be seen implemented from the meetings and training, as mentioned in the first layer. As Parsons (2010) underlines, there is no guarantee that the values and beliefs will lead to some shared assumption. For instance, while the Microsoft Authenticator App is the recommended method, several employees refrain from utilizing it. This demonstrates how some employees interpret this assertion from management as an expression of a value to be challenged and confronted. Another example is how no interviewee recalled the Motimate course concerning 2FA, though it is supposed to be mandatory. This makes it difficult to know if the guidelines provided in the course were something the interviewees implemented in their behavior in later practice.

The third and last layer of Schein and Schein’s (2016) model are shared basic assumptions. As Parsons (2010) explains, these are invisibly embedded, making them difficult to observe and evaluate. With the scope of our survey and interviews, we should be careful making conclusions about the underlying and unconscious perceptions, thoughts and feelings of employees.

Still, we can observe some of these basic assumptions as the lack of variation within the social unit. For instance, every interviewee perceives cybersecurity as important and central in the organization. Furthermore, interviewees conveyed that they presume their colleagues share the same belief, and we have reason to believe that any divergence from this shared belief and values would be deemed inconceivable by them. The importance of cybersecurity is perceived by the respondents as a non-debatable and non-comfortable value, unlike the values and beliefs in the second layer. Another example that displays these shared basic expressions is how the interviewees reacted to the implementation of number matching in the Microsoft Authenticator App - it was unquestioned, because they agreed that it increased security. Another aspect of the shared basic assumptions of the cybersecurity culture in Atea is that they provide a sense of identity for the employees. When discussing cybersecurity, the interviewees found belonging, self-esteem and safety in their relations to their colleagues and the organization. Also, the trust and commitment in these relations may be why the survey respondents strongly agree to the statement that they notify their employer immediately if they discover a security breach with their work account.

Schein and Schein’s (2016) model can be used to describe and analyze the cybersecurity culture of Atea, but also the individual employee’s cultural identity. No discernible subcultures have been observed; rather, it appears that Atea employees identify themselves with the organization's community as a whole. The individual employee identifies with the shared values and shared basic assumptions of their teams, departments and the company.

As highlighted by AlHogail and Mirza’s (2014) definition, cybersecurity culture should materialize in some wanted behavior among the employees. Specifically, the authors write that acting secure should be “second nature” for the employees. The interviewees mostly acted secure in the way that they use 2FA as intended in their work. The majority use the Microsoft Authenticator App, and avoided considerable alternative solutions, despite encountering occasional challenges during the authentication process. The interviewees also mostly described their relationship to cybersecurity in ways that could be interpreted as second nature. The interviewees were aware of their own habits and behavior regarding cybersecurity and 2FA, yet without feeling that it was strained or enforced.

This behavior of the interviewees can further be contextualized in the cybersecurity culture of the organization, as suggested by Sample et al. (2018). The authors suggest that cultural values for information security determine the norm of the group. As mentioned earlier, curiosity and responsibility are formally some of Atea’s values that they strive to maintain among their employees. Additionally, as also seen from Schein and Schein’s (2016) model, the interviewees seem to align with several of the same values. This can be seen from their beliefs and perceptions about the importance of cybersecurity, which is also communicated from management. The interviewees also often explain their own personal knowledge about cybersecurity and attitudes toward 2FA by contextualizing it to the team they are a part of. Furthermore, the interviewees often refer to their knowledge to justify and explain their positive attitudes toward 2FA, and in that way reflecting group norms and influence to personal qualities and perceptions, ultimately shaping individual user experiences of technology. The values and group norms can also be seen materialized in the employees’ commitment to organizational compliance.

Further, Glaspie and Karwowski (2018) describe how there is a mutual influence, as users’ experiences alter their perceptions and attitudes toward cybersecurity. At the same time, employees' attitudes and involvement in cybersecurity compliance, impact the cybersecurity culture in the organization. This can be seen from the results, as both the respondents from the survey and interviewees paint a positive picture of their personal commitment and feelings toward 2FA as a cybersecurity measure, as well as their perception of the overall cybersecurity culture. A positive culture can also be seen in their positive perception of colleagues' competencies and their behavioral intent, and the knowledge sharing occurring between colleagues.

5.3.1 Training

Theory suggests that adequate organizational cybersecurity training has the potential to enhance the human aspect of security (Bishop, 2003; Parsons, 2010; Sample et al., 2018). Given that 2FA is not a purely technical implementation, but used and handled by employees and customers of Atea, it is evident that they should strive to eliminate potential human errors. It is essential that employees are properly trained in the use of security measures, like 2FA, to ensure that they understand its importance and have sufficient knowledge to use it effectively to protect sensitive data and systems. We will now describe some important aspects to consider while implementing training in Atea.

Glaspie and Karwowski and Parsons (2018; 2010) emphasized how training should focus on meeting the individual users at their level of competencies. Although Atea offers many training programs covering diverse aspects of cybersecurity, in regard to authentication specifically, this is not the case. For instance, employees that do not know about the Microsoft Authenticator App, or have not gotten it to work, neither sought nor found an easy and suitable resource to address their issues. This lack of action may be attributed to their perception that their lack of knowledge is not a significant issue. However, given that Atea's objective is to promote the use of the app, the organization should explore relevant training options to support these employees. This way Atea also bridges the gap between the need of their employees and their security policies, as the authors emphasize. However, for the majority of employees that do use the app regularly, that do not experience significant issues and do have a good understanding of 2FA as a cybersecurity measure, there should be other training options.

Further, training should be relevant to individual user experiences (McBride et al., 2012), meaning that Atea should assess their employees' personalities and develop customized training programs to suit the needs of each employee. For instance, it was mentioned by several interviewees how older users tend to have a harder time than younger users in understanding technology and how rapidly it evolves. This is potentially more relevant to certain customers, as the average age at Atea is relatively low. This approach has the potential to foster a culture where all employees have access to the necessary training. This training should also stimulate individual awareness that fosters a culture to reinforce the wanted behavior. The content of the training should be updated as the assumptions change.

According to the authors (Glaspie & Karwowski, 2018; Parsons, 2010), training should involve learning the impact of a security incident. This practice is shown to be effective in increasing awareness and is an important part of training that Atea should consider incorporating in their training programs. We have learned that Atea has a 2FA course in Motimate and has done a phishing test on their employees, but more extensive tests and training should be done, as the majority of the interviewees could not recollect receiving any training.

5.4 Our Contribution and Recommendations

Comparing findings from previous literature to the findings of our research, it is evident that they are largely supportive of each other. We have not found any significant disparities between our study's descriptions of the user experience of 2FA and those presented in other case studies by different authors. The challenges that are identified in our case are also observed in other studies. The main contribution of our research however, and how it differs from previous researched cases, is how it studies the implementation of 2FA in an IT company specifically. Previous case studies have examined 2FA in non-technical organizations. As an organization specializing in information technology and information security, Atea and its employees possess distinct qualities and attributes in these areas. That is why outlining their internal cybersecurity culture was seen as important for understanding the user experience of 2FA among their employees. Atea has a very strong and positive cybersecurity culture, and the employees have higher than average competencies, knowledge and awareness concerning these concepts. The respondents themselves refer to these qualities and values when explaining their user experience of 2FA. This is also seen in their perspective on 2FA as a security mechanism and their motivations for using it. Namely, though they appreciate 2FA because of the security benefits they know it provides, they will to a higher degree tolerate the challenges that come with it.

For Atea, the research presented in this thesis can be a valuable contribution in several respects. Firstly, Atea may choose to conduct further internal surveys beyond Region Nord to verify and delve deeper into the outcomes of the research and evaluate their organizational cybersecurity culture more comprehensively. Secondly, based on relevant factors from the research findings, Atea can formulate best practices for creating or enhancing their cybersecurity culture. We would also recommend management of Atea to encourage employees to individually be aware of security risks, also outside of the company. Lastly, Atea can take measures to provide their employees with a more streamlined user experience of 2FA, thereby improving their overall work experience with 2FA.

These measures could include a more enhanced training program and -options for both authentication as a cybersecurity measure and the practical utilization of 2FA. This could be implemented in the courses they already have in their internal training platform, Motimate. Similarly, Atea should ensure that the Microsoft Authenticator App is known to every employee, and that those who encounter issues with its use can easily access user support. Further, our research suggests some design implications for Microsoft’s 2FA-technology that would improve the user experience, such as improving their SSO solution and reducing technical errors. Although these issues are out of Atea’s control, as customers and users of Microsoft, they should be aware of them in order to gain understanding of the challenges their employees encounter. If Microsoft develop new and more seamless 2FA, Atea should not hesitate in implementing these solutions. However, in conclusion, Atea should keep doing what they have already established in their organization to improve the cybersecurity culture, as it has proven successful. This is reflected in the employee’s positive experience with 2FA.

5.5 Weaknesses

This thesis is based on a case study from a specific regional department of an IT consultancy firm. While a case study gave some favorable qualities to the research and allowed for an in-depth exploration of the topic, it also presents challenges in generalizing the findings to other types of organizations. For instance, it would be very interesting to research the customers of Atea Region Nord. Many of them are vastly different organizations to Atea, like municipalities and state enterprises, that operate under completely different and distinct conditions. In these organizations, user experience of 2FA and cybersecurity culture may be less of explicit focus, yet should hold an equal importance.

Further, both the number of interviews and the diversity of interviewees could be seen as a weakness with the research. To enhance the breadth of knowledge within the scope of the research, as a case study of an IT firm, it would be beneficial with a selection of interviewees with more diverse expertise and from varying hierarchical positions in the organization. As an example, it would be compelling to conduct an interview with someone from higher-level management, to obtain valuable strategic and leadership insights on these topics.

5.6 Future Work

In this thesis we present findings concerning the user experience of 2FA, the challenges users encounter, and how this phenomenon occurs in the context of an organizational cybersecurity culture. These findings can serve as metrics to create more user-friendly 2FA solutions. Moreover, the findings can help understand users' perceptions of cybersecurity measures, and improve the facilitation of user adoption of these measures. Ultimately, this can lead to more successful implementation of cybersecurity measures.

For future research on these issues, it would be recommended to study the identified factors further to validate the findings presented in this thesis, and to examine their applicability in diverse contexts. If this thesis had a longer time span, it would be ideal to interview a more extensive sample of employees and from various companies, not only IT specialists. More thorough surveys and observations could be done. Additionally, new factors related to both the UX of security measures and cybersecurity culture may be identified, as well as other connections to this mutual relation and their impact. Future research should also aim to develop and establish best practices for ensuring secure and compliant employee conduct and to foster a favorable cybersecurity culture.

6 Conclusion

Based on the data collected, the study provides insights into how users perceive and experience two-factor authentication in Microsoft 365. The user experience of 2FA extends beyond just usability and encompasses various factors that influence the process during and after authentication. These factors may include encountered challenges, motivations, training, and the overall cybersecurity culture within the organization. The interplay of these conditions, among others, shapes employees' attitudes toward and engagement with 2FA. Although 2FA is mandatory in the studied case company, Atea, it is still important to keep employees motivated to use it. By understanding the values and benefits of this security mechanism, employees are more likely to have a satisfactory interaction with 2FA.

Previous research has investigated the user experience of 2FA at various universities and in non-technical companies where cybersecurity is not the core business and therefore not a natural part of their tasks. In contrast, our study focuses on an IT company, where employees' perception of 2FA is likely to differ due to the nature of their work. Understanding the holistic user experience of 2FA requires consideration of multiple factors. However, identifying how to improve the usage can be challenging, and this may be one reason why some companies have not yet implemented 2FA. Our case study sheds light on the interrelationship between various factors that contribute to the overall user experience. As employees are the primary users of the 2FA system, it is vital that the system meets their needs. People tend to opt for the easier path, and if 2FA fails to meet users' expectations and leave them with a positive perception, users may want the simpler option, like SFA.

If we reflect on the research questions that were defined in chapter 1, we can establish connections between the sub-research questions and the main research question, which is "*How is two-factor authentication experienced by users in Microsoft 365?*". Our research has identified the primary challenges associated with 2FA, including frequent authentication requests, illogical 2FA, and technical errors. We have also explored why employees encounter these challenges, such as the tasks included in their daily work and lack of training, and how the cybersecurity culture at Atea plays a role in shaping their experiences. This culture encompasses factors such as shared values, the sense of community, knowledge sharing, and personal qualities, like skepticism and attentiveness, all of which can affect the overall user experience of 2FA in some way. Different issues, such as technical issues, can lead to poor usability of the service, which in turn can result in an unsatisfactory user experience. Conversely, fewer challenges and a positive cybersecurity culture can contribute to a more satisfactory user experience. By discussing these research questions in this thesis, we have provided clarity on these relationships.

Recognizing the challenges that users face with 2FA and finding solutions to avoid them is of utmost importance. Furthermore, fostering a cybersecurity culture that promotes satisfaction among employees will enhance their competencies and knowledge. This can lead to a positive user experience with 2FA. Developing a good cybersecurity culture can help employees gain the necessary competencies and knowledge, which employees have said to be a reason for their satisfying user experience. In turn, their competencies and knowledge can promote a positive cybersecurity culture. Ongoing evaluation and identification of best practices for the use of 2FA can lead to an increasingly positive user experience.

In general, employees express satisfaction with the use of 2FA, recognizing its importance as a security benefit. However, it is worth noting how management can support employees in achieving a satisfying user experience of 2FA. Strategies such as reducing the frequency of requests, enabling 2FA only when necessary, and providing technical assistance can enhance the user experience. Particularly now that remote work has become more common, reducing the frequency of requests is especially a priority. The feeling of adequate training in 2FA was found to have only a small correlation with how employees perceive the app's usability, as indicated by the small coefficient of 0.161. Providing more training can therefore guide employees to perceive the Microsoft Authenticator App as usable and adopt it, as it is the safest option for 2FA at work. It is important to keep employees motivated to use 2FA and to ensure they understand its significance, while also promoting a positive cybersecurity culture. These efforts may lead to even greater satisfaction among employees regarding the user experience of 2FA, ultimately enhancing the company's overall security.

References

Abbott, J., & Patil, S. (2020). How Mandatory Second Factor Affects the Authentication User Experience. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376457

Acemyan, C. Z., Kortum, P., Xiong, J., & Wallach, D. S. (2018). 2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *62*(1), 1141–1145. https://doi.org/10.1177/1541931218621262

Al Mehairi, A., Zgheib, R., Abdellatif, T. M., & Conchon, E. (2022). Cyber Security Strategies While Safeguarding Information Systems in Public/Private Sectors. I F. Ortiz-Rodríguez, S. Tiwari, M.-A. Sicilia, & A. Nikiforova (Red.), *Electronic Governance with Emerging Technologies* (s. 49–63). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-22950-3_5

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 1–7. https://doi.org/10.1109/WCCAIS.2014.6916579

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, *40*(3), 1153–1166. https://doi.org/10.32604/csse.2022.019938

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Bd. Second edition*. Syngress. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=786214&site=ehost-live&scope=site

Berg, B. L., & Lune, H. (2017). *Qualitative research methods for the social sciences* (Ninth edition). Pearson.

Bevan, N. (2009a). *What is the difference between the purpose of usability and user experience evaluation methods?*

Bevan, N. (2009b). *What is the difference between the purpose of usability and user experience evaluation methods?*

Bishop, M. (2003). What is computer security? *IEEE Security & Privacy*, *1*(1), 67–69. https://doi.org/10.1109/MSECP.2003.1176998

Boehm, J., Kaplan, J., & Richter, W. (2020). *Safeguarding against cyberattack in an increasingly digital world*. McKinsey. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/safeguarding-against-cyberattack-in-an-increasingly-digital-world

Bonneau, J., & Preibusch, S. (2010). *The password thicket: Technical and market failures in human authentication on the web*.

Busch, T. (2016). *Akademisk skrivning for bachelor- og masterstudenter*.

Ciolino, S., Parkin, S., & Dunphy, P. (2019). *Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling*.

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018). "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–11. https://doi.org/10.1145/3173574.3174030

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The Tangled Web of Password Reuse. *Proceedings 2014 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA. https://doi.org/10.14722/ndss.2014.23357

Das, S., Dingman, A., & Camp, L. J. (2018). Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key. I S. Meiklejohn & K. Sako (Red.), *Financial Cryptography and Data Security* (s. 160–179). Springer. https://doi.org/10.1007/978-3-662-58387-6_9

Dasgupta, D., Roy, A., & Nag, A. (2017). Multi-Factor Authentication. I D. Dasgupta, A. Roy, & A. Nag (Red.), *Advances in User Authentication* (s. 185–233). Springer International Publishing. https://doi.org/10.1007/978-3-319-58808-7_5

De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2014). *A Comparative Usability Study of Two-Factor Authentication* (arXiv:1309.5344). arXiv. http://arxiv.org/abs/1309.5344

Dourish, P., Grinter, R. E., Delgado de la Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*(6), 391–401. https://doi.org/10.1007/s00779-004-0308-5

Dutson, J., Allen, D., Eggett, D., & Seamons, K. (2019). Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 119–128. https://doi.org/10.1109/EuroSPW.2019.00020

ENISA. (2017). Cyber Security Culture in organisations. *European Union Agency For Network and Information Security*.

EU. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*. Hart Publishing. https://doi.org/10.5040/9781782258674

Evans, M., He, Y., Maglaras, L., Yevseyeva, I., & Janicke, H. (2019). Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. *International Journal of Medical Informatics*, *127*, 109–119. https://doi.org/10.1016/j.ijmedinf.2019.04.019

Fassl, M., Gröber, L. T., & Krombholz, K. (2021). Exploring User-Centered Security Design for Usable Authentication Ceremonies. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–15. https://doi.org/10.1145/3411764.3445164

Gatlan, S. (2023, mai 8). *Microsoft enforces number matching to fight MFA fatigue attacks*. BleepingComputer. https://www.bleepingcomputer.com/news/microsoft/microsoft-enforces-number-matching-to-fight-mfa-fatigue-attacks/

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Security Journal*, *35*(2), 486–505. https://doi.org/10.1057/s41284-021-00286-2

Glaspie, H. W., & Karwowski, W. (2018). Human Factors in Information Security Culture: A Literature Review. I D. Nicholson (Red.), *Advances in Human Factors in Cybersecurity* (s. 269–280). Springer International Publishing. https://doi.org/10.1007/978-3-319-60585-2_25

Golla, M., Ho, G., Lohmus, M., Pulluri, M., & Redmiles, E. M. (2021). *Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns*.

Grillenmeier, G. (2021). Now's the time to rethink Active Directory security. *Network Security*, *2021*(7), 13–16. https://doi.org/10.1016/S1353-4858(21)00076-3

Grimes, R. (2019). The many ways to hack 2FA. *Network Security*, *2019*(9), 8–13. https://doi.org/10.1016/S1353-4858(19)30107-2

Gulbrandsen, A. (2017, april 10). *Informasjonssikkerhet og risikovurdering for Nettskjema—Universitetet i Oslo*. UiO. https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/informasjonssikkerhet/index.html

Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011a). *User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking | Elsevier Enhanced Reader*. https://doi.org/10.1016/j.cose.2010.12.001

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

Hilliger, I., Muñoz-Merino, P. J., De Laet, T., Ortega-Arranz, A., & Farrell, T. (Red.). (2022). *Educating for a New Future: Making Sense of Technology-Enhanced Learning Adoption: 17th European Conference on Technology Enhanced Learning, EC-TEL 2022, Toulouse, France, September 12–16, 2022, Proceedings* (Bd. 13450). Springer International Publishing. https://doi.org/10.1007/978-3-031-16290-9

Hmelo-Silver, C., Chinn, C., Chan, C., & O'Donnell, A. (2013). *The International Handbook of Collaborative Learning*. Routledge.

Hofstede, G. H., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind: intercultural cooperation and its importance for survival* (3rd ed). McGraw-Hill.

Isenberg, P., Elmqvist, N., Scholtz, J., Cernea, D., Ma, K.-L., & Hagen, H. (2011). Collaborative visualization: Definition, challenges, and research agenda. *Information Visualization*, *10*(4), 310–326. https://doi.org/10.1177/1473871611412817

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser?: Innføring i samfunnsvitenskapelig metode* (2. utgave). Høyskoleforlaget.

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2011). *Forskningsmetode for økonomisk-administrative fag*.

Kirlappos, I., & Sasse, M. A. (2014). What Usable Security Really Means: Trusting and Engaging Users. I T. Tryfonas & I. Askoxylakis (Red.), *Human Aspects of Information Security, Privacy, and Trust* (s. 69–78). Springer International Publishing. https://doi.org/10.1007/978-3-319-07620-1_7

Kocksch, L., Korn, M., Poller, A., & Wagenknecht, S. (2018). Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 92:1-92:20. https://doi.org/10.1145/3274361

Lal, N. A., Prasad, S., & Farik, M. (2016). *A Review Of Authentication Methods*. *5*(11).

Lennartsson, M., Kävrestad, J., & Nohlberg, M. (2021). Exploring the meaning of usable security – a literature review. *Information & Computer Security*, *29*(4), 647–663. https://doi.org/10.1108/ICS-10-2020-0167

Malmedal, B., & Røislien, H. E. (2016). *The Norwegian Cyber Security Culture*. Norwegian Centre for Information Security (NorSIS).

Mancuso, V. F., Strang, A. J., Funke, G. J., & Finomore, V. S. (2014). Human Factors of Cyber Attacks: A Framework for Human-Centered Research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *58*(1), 437–441. https://doi.org/10.1177/1541931214581091

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

McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies. *RTI International*.

Mirkovic, J. (2010). *Report: Main factors affecting user acceptance of authentication methods for mobile services in Norway*. UiO, Department of Informatics.

Nag, A. K., Roy, A., & Dasgupta, D. (2015). An Adaptive Approach Towards the Selection of Multi-Factor Authentication. *2015 IEEE Symposium Series on Computational Intelligence*, 463–472. https://doi.org/10.1109/SSCI.2015.75

Nettskjema. (u.å.). Hentet 12. mai 2023, fra https://nettskjema.no

Nirmal, J. R., Kiran, R. B., & Hemamalini, V. (2022). Improvised multi-factor user authentication mechanism using defense in depth strategy with integration of passphrase and keystroke dynamics. *Materials Today: Proceedings*, *62*, 4837–4843. https://doi.org/10.1016/j.matpr.2022.03.439

NSA. (2020). *Selecting Secure Multi-factor Authentication Solutions*. National Security Agency.

NSD. (2021). *Strukturendring i kunnskapssektoren*. NSD. https://nsd.no/artikkel/strukturendring-i-kunnskapssektoren/

Oates, B. J., Griffiths, M., & McLean, R. (2022). *Researching Information Systems and Computing (Second Edition)*. Sage Publications Ltd.

Ogie, R. I., James, S., Moore, A., Dilworth, T., Amirghasemi, M., & Whittaker, J. (2022). *Social media use in disaster recovery: A systematic literature review | Elsevier Enhanced Reader*. https://doi.org/10.1016/j.ijdrr.2022.102783

Orellana, S. (2017). Digitalizing Collaboration. *Research-Technology Management*, *60*(5), 12–14. https://doi.org/10.1080/08956308.2017.1348125

Parsons, K. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment*.

Quintão, C., Andrade, P., & Almeida, F. (2020). How to Improve the Validity and Reliability of a Case Study Approach? *Journal of Interdisciplinary Studies in Education*, *9*(2), Artikkel 2. https://doi.org/10.32674/jise.v9i2.2026

Rajesh, L. (2022). *DESIGN AND DEVELOPMENT OF AN INTEGRATED FRAME WORK FOR SECURE COMMUNICATION PROTOCOL IN INDUSTRIAL CONTROL SYSTEMS*. http://ir.kluniversity.in/xmlui/bitstream/handle/123456789/740/80_recommendation.pdf?sequence=18&isAllowed=y

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). *A Usability Study of Five Two-Factor Authentication Methods*.

Reynolds, J., Smith, T., Reese, K., Dickinson, L., Ruoti, S., & Seamons, K. (2018). A Tale of Two Studies: The Best and Worst of YubiKey Usability. *2018 IEEE Symposium on Security and Privacy (SP)*, 872–888. https://doi.org/10.1109/SP.2018.00067

Saini, D. K., Kumar, K., & Gupta, P. (2022). Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions. *Security and Communication Networks*, *2022*, e4943225. https://doi.org/10.1155/2022/4943225

Salopek, J. J. (2000). Digital Collaboration. *Training &amp; Development*, *54*(6), 38–38.

Sample, C., Cowley, J., Hutchinson, S., & Bakdash, J. (2018). Culture + Cyber: Exploring the Relationship. I D. Nicholson (Red.), *Advances in Human Factors in Cybersecurity* (s. 185–196). Springer International Publishing. https://doi.org/10.1007/978-3-319-60585-2_18

Schein & Schein. (2016). *Organizational Culture and Leadership: Bd. Fifth edition*. Wiley.

Schneier, B. (Red.). (2003). Identification, Authentication, and Authorization. I *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (s. 181–206). Springer. https://doi.org/10.1007/0-387-21712-6_13

Schneier, B. (2015). *Secrets and lies: Digital security in a networked world* (Fifteenth Anniversary Edition). John Wiley & Sons, Inc.

Stanislav, M. (2015). *Two-Factor Authentication*. IT Governance Ltd.

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*, 483–487. https://doi.org/10.1016/j.procs.2022.12.050

Theofanos, M. (2020). Is Usable Security an Oxymoron? *Computer*, *53*(2), 71–74. https://doi.org/10.1109/MC.2019.2954075

Tjora, A. (2019). *Qualitative research as stepwise-deductive induction* (Bd. 26). Routledge.

Tolone, W., Ahn, G.-J., Pai, T., & Hong, S.-P. (2005). Access control in collaborative systems. *ACM Computing Surveys*, *37*(1), 29–41. https://doi.org/10.1145/1057977.1057979

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, *2*(3), Artikkel 3. https://doi.org/10.3390/jcp2030029

Tsang, E. W. K. (2014). Generalizing from Research Findings: The Merits of Case Studies. *International Journal of Management Reviews*, *16*(4), 369–383. https://doi.org/10.1111/ijmr.12024

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N., & Cranor, L. F. (2015). *"I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab*.

Violino, B. (2020, desember 14). *How to manage multiple cloud collaboration tools in a WFH world*. Computerworld. https://www.computerworld.com/article/3584538/how-to-manage-multiple-cloud-collaboration-tools-in-a-wfh-world.html

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Weinert, A. (2019). *Your Pa$word doesn't matter*. Microsoft. https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984

Weir, C. S., Douglas, G., Richardson, T., & Jack, M. (2010). Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers*, *22*(3), 153–164. https://doi.org/10.1016/j.intcom.2009.10.001

Whitten, A., & Tygar, J. D. (1999). *WHY JOHNNY CAN'T ENCRYPT: A USABILITY EVALUATION OF PGP 5.0*.

World Economic Forum. (2022). *Global Risks Report 2022*. https://www.weforum.org/reports/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/

Yee, K.-P. (2004). Aligning security and usability. *IEEE Security & Privacy*, *2*(5), 48–55. https://doi.org/10.1109/MSP.2004.64

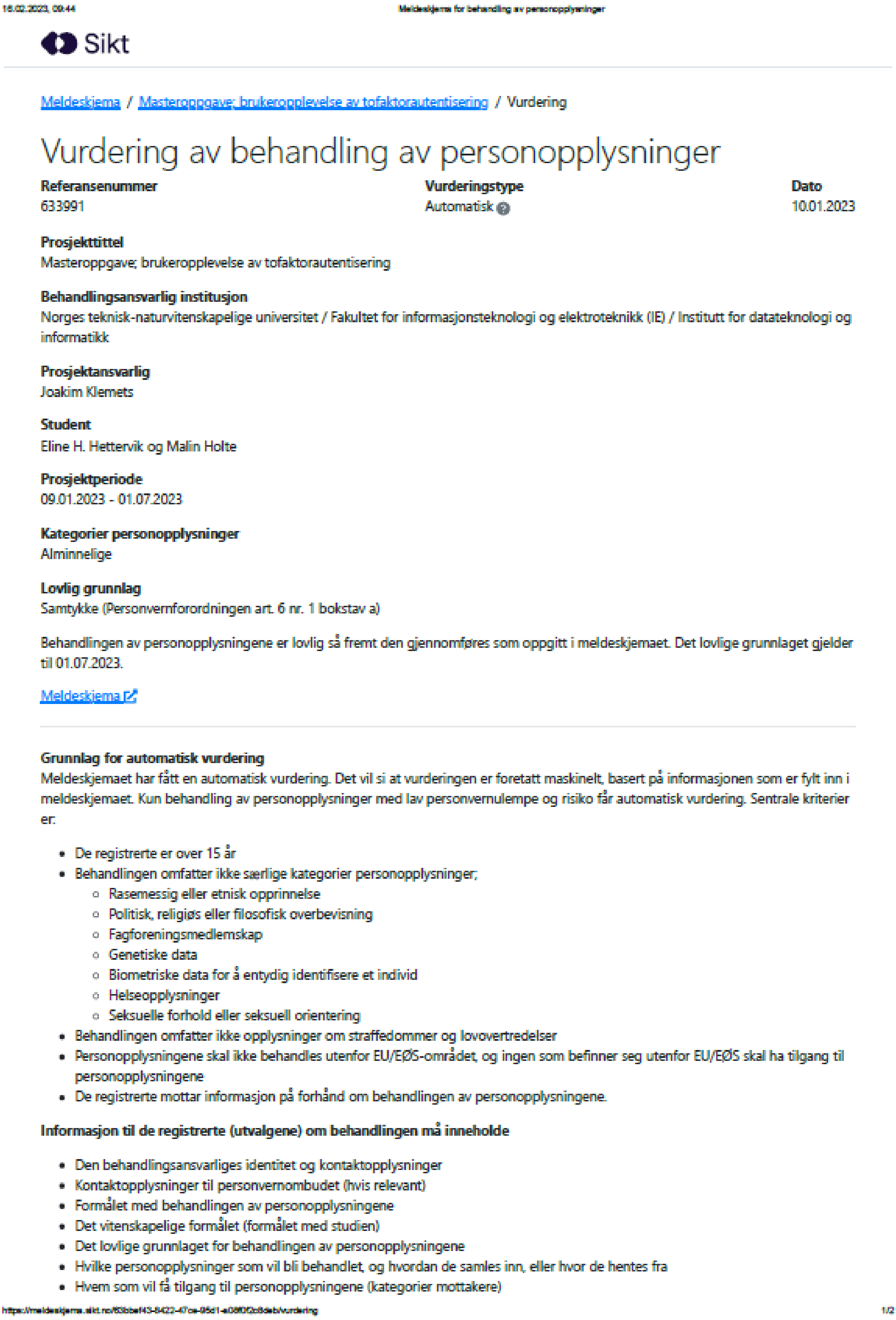
Yin, R. K. (2009). *Case Study Research: Design and Methods* (Bd. 4). Sage Publications Ltd.

Zinda, Z. (2021, oktober 4). *Data Science Stats Review: Pearson's, Kendall's, and Spearman's Correlation for Feature Selection*. PhData. https://www.phdata.io/blog/data-science-stats-review/

Zwane, Z. P., Mathonsi, T. E., & Maswikaneng, S. P. (2021). An Intelligent Security Model for Online Banking Authentication. *2021 IST-Africa Conference (IST-Africa)*, 1–6.

Appendix

A Application to NSD



Sikt

Meldeskjema / Masteroppgave; brukeropplevelse av tofaktorautentisering / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
633991	Automatisk ?	10.01.2023

Prosjekttittel
Masteroppgave; brukeropplevelse av tofaktorautentisering

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for datateknologi og informatikk

Prosjektansvarlig
Joakim Klemets

Student
Eline H. Hettervik og Malin Holte

Prosjektperiode
09.01.2023 - 01.07.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 01.07.2023.

Meldeskjema

Grunnlag for automatisk vurdering
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

Informasjon til de registrerte (utvalgene) om behandlingen må inneholde

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)

- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

Informasjonssikkerhet
Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.

B Consent Form for Interviews

Vil du delta til masteroppgaven

The user experience of two-factor authentication in digital collaboration tools?

Dette er et spørsmål til deg om å delta som informant til vår masteroppgave som handler om brukeropplevelsen av tofaktorautentisering i Microsoft 365. Formålet med dette intervjuet er å samle informasjon om hva dine erfaringer og opplevelser er av dette i din arbeidshverdag. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Denne masteroppgaven er en del av masterstudiet Digital Samhandling ved NTNU Trondheim. Masteroppgaven tilsvarer 30 stp. og skal skrives ferdig våren 2023. Problemstillingen for oppgaven, som vi skal forsøke å besvare gjennom datainnsamling og -analyser, er "How is two-factor authentication as a security mechanism experienced by users in M365?" (Hvordan blir tofaktorautentisering som en sikkerhetsmekanisme opplevd av brukere i M365). I forlengelse av dette har vi flere delproblemstillinger som handler om utfordringer med tofaktorautentisering og hvordan brukeropplevelser gir ringvirkninger for den mer overhengende sikkerhetskulturen i organisasjonen.

Det har i forskning blitt økt fokus på viktigheten av positive brukeropplevelser for gode sikkerhetsmekanismer som fungerer optimalt. Dette ses i forskningsfeltet som kalles Usable Security. Likevel har tidligere studier ikke nødvendigvis vist hvor viktig dette er, og hvordan det gir ringvirkninger for en kollektiv sikkerhetskultur i organisasjoner. Dette er noe vi ønsker å utforske og besvare gjennom denne masteroppgaven.

Hvem er ansvarlig for forskningsprosjektet?

- Eline Hagen Hettervik og Malin Holte
- NTNU, Institutt for datateknologi og informatikk.
- Atea. Masteroppgaven blir skrevet i samarbeid med Atea. Atea foreslo temaet brukeropplevelse av sikkerhetsmekanismer, og den spesifikke problemstillingen ble utarbeidet av studentene, veileder, og våre kontaktpersoner i Atea. Atea bidrar med informanter og veiledning til oppgaven. Atea får ikke tilgang til rådata, men vil få tilgang til den endelige oppgaven. Det vil bli holdt en presentasjon av resultatene fra oppgaven etter innleveringsfrist, som vil være åpen for alle i Atea Region Nord å delta på.

Hvorfor får du spørsmål om å delta?

Du blir spurt om å delta fordi du jobber i Atea og har erfaring med bruk av tofaktorautentisering i M365 i ditt arbeid. Vi har blitt satt i kontakt med deg via HR-sjefen i Atea.

Hva innebærer det for deg å delta?
Hvis du velger å delta i dette prosjektet, innebærer det at du svarer på noen spørsmål i et intervju (ca. 30-60 minutt). Intervjuet vil inneholde spørsmål om dine holdninger rundt tofaktorautentisering som sikkerhetsmekanisme. Svarene dine vil bli lagret på lydopptak (evt video hvis vi tar det digitalt) i OneDrive, som kun vi studentene og prosjektansvarlig har tilgang til.

Det har tidligere blitt sendt ut et spørreskjema fra oss til alle i Atea Region Nord. Dette spørreskjemaet er helt anonymt. Spørreskjemaet er laget i Nettskjema, utviklet av UiO, og anbefalt av NTNU for sikker løsning for datainnsamling. Svarene du evt. ga i dette spørreskjemaet, er helt anonyme, og knyttes ikke til det du sier i dette intervjuet.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- De som har tilgang til dine opplysninger vil være forfatterne av masteroppgaven Eline Hettervik og Malin Holte og veileder Joakim Klemets ved NTNU.
- Uvedkommende får ikke tilgang til personopplysningene dine. Opplysningene dine lagres sikkert på OneDrive bare forfatterne av masteroppgaven har tilgang til. I behandlingen av dataen og i den endelige masteroppgaven vil opplysningene dine bli anonymisert. OneDrive er anbefalt av NTNU til lagring av personopplysninger, og annen åpen, intern og fortrolig informasjon.
- Programvaren til transkripsjon er Word og Teams. Transkripsjonene blir lagret i OneDrive.

Deltakere i intervjuet vil ikke kunne gjenkjennes i masteroppgaven. Opplysningene som vil publiseres er anonymisert statistikk, i tillegg til beskrivelse av eller sitat fra intervjuet som er relevant til problemstillingen, men vil ikke kunne knyttes til en person.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes i juni 2023. Etter prosjektslutt vil datamaterialet med dine personopplysninger slettes.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har Sikt – Kunnskapssektorens tjenesteleverandørs personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- NTNU ved Eline Hettervik (elinehh@ntnu.no) og Malin Holte (maliholt@ntnu.no) (forfattere av masteroppgaven), NTNU ved Joakim Klemets (joakim.klemets@ntnu.no) (veileder for masteroppgaven) eller Atea ved Terje André Tronstad (Terje.Andre.Tronstad@atea.no) (kontaktperson i Atea).
- Vårt personvernombud ved NTNU: Thomas Helgesen (thomas.helgesen@ntnu.no)

Hvis du har spørsmål knyttet til vurderingen av prosjektet som er gjort av Sikts personverntjenester ta kontakt på:

- Epost: personverntjenester@sikt.no, eller telefon: 53 21 15 00.

Med vennlig hilsen

Prosjektansvarlig: Terje André Tronstad
Studenter: Eline Hagen Hettervik og Malin Holte
Veileder: Joakim Klemets

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet masteroppgaven “The user experience of two-factor authentication in digital collaboration tools” og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet.

(Signert av prosjektdeltaker, dato)

C Interview Guide

Intervjuguide

Problemstilling; How is two factor authentication as a security mechanism experienced by users in M365?

Har du skrevet under på samtykkeskjemaet?

Fase 1: Rammesetting	**Løs prat** • Uformell prat • Introduksjon av oss og masteroppgaven • Spørre om samtykkeskjema og starte opptak **Informasjon** • Forklarer samarbeidet med Atea • Forklarer bakgrunn og formål for intervjuet • Introdusere problemstilling • Målet med intervjuet: bli kjent med informantens rolle i Atea, informantens erfaringer, tanker og meninger om temaene. • Forklarer hvordan informanten står fritt til å svare, gjenta seg selv, gå utenfor scopet på spørsmålet og trekke seg når som helst. • Oppklare uklarheter (si at vi spør i jobbsammenheng mtp 2FA i Microsoft) og spørsmål fra informanten. • Informere om opptak, få samtykke til opptak og starte opptak (Teams + Nettskjema).
Fase 2: Bakgrunn	**Overgangsspørsmål** 1. Hvilken avdeling jobber du i og hvilken stilling/rolle har du? 2. Jobber du med IT-sikkerhet og i så fall på hvilken måte? 1. Hvor bevisst er du på sikkerhet i ditt eget digitale arbeid? [lagt til etter intervju 3] 3. Hvilken metode bruker du på jobb for å tofaktorautentisere deg?
Fase 3: Fokusering	**Nøkkelspørsmål** **Opplæring og sikkerhetskultur** 1. Hva synes du om opplæringen dere får på jobb i tofaktorautentisering? 2. Hvordan synes du set-up prosessen var for tofaktorautentisering på jobb?[fjerna etter intervju 3] 3. Hvordan synes du kulturen er for IT-sikkerhet på jobben? 4. Hvilke egenskaper hos ansatte bidrar til god kultur for IT-sikkerhet? **Tofaktor, utfordringer og motivasjon** 5. Synes du det er forskjell på de ulike måtene du kan tofaktorautentisere deg på i jobben? 1. Hvilken liker du best? 2. Hvordan liker du den nye måten med number matching i forhold til den gamle?

	6. Hvor mange ganger i løpet av en jobbdag må du tofaktorautentisere deg? 1. Føler du at antall ganger er for ofte? 7. Synes du det er behov for tofaktor og i hvilke tilfeller synes du ikke det er behov for tofaktor? 1. Kan du se for deg en bedre løsning? 8. Opplever du utfordringer med tofaktorautentisering i M365 og i så fall hvorfor tror du at du opplever disse? 1. Har du noen gang opplevd tofaktorautentisering i M365 som et hinder for effektivitet, produktivitet eller lignende? I så fall på hvilken måte? 9. Opplever du tofaktorautentisering i M365 som annerledes enn andre tofaktorautentiseringsløsninger som du har brukt (for eksempel privat)? 10. Hva gjør du hvis du synes tofaktor er for tungvint og hva tror du er konsekvensene av dette? 11. Hva er motivasjonen din for å bruke tofaktor? 1. Føler du at fordelene veier opp for utfordringene? **Kunder** 12. Har du vært med å implementere tofaktor hos en kunde? 1. I så fall: Hva tror du er opplevelsen til kundene av tofaktorautentisering i M365?
Fase 4: Oppsummering	**Oppsummering** • Oppsummere funnene • Har vi forstått objektet riktig? • Er det noe objektet vil legge til? • Stoppe opptak

D Survey Average Value Calculation Explanation

Calculating the average score (between 1-5) in section two and three of the survey was done in the following way: the answer options got a number from 1-5, where “strongly disagree” was assigned 1 and “strongly agree” was assigned 5, as can be seen from table D.1 and D.2. We then multiplied the amount of answers on each of these options for S1-S9 and S1-S6 with a number from 1-5. The statements are in the order as they appear in the survey. The summation of the numbers for each statement was divided by the total number of respondents on that statement. These answers were between 1-5, and represented the average score for each statement. We omitted the respondents that answered “I don’t know/not relevant”. In the first table these were only 17 answers out of 1008 (i.e. 112 employees * 9 statements) total answers across all the statements. In the second table these were only 14 out of 732 (122 employees * 6 statements). This omission is the reason why the number of respondents on each statement varies - depending on how many answered “I don’t know/not relevant” on each statement.

Statements	1 Strongly disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly agree	Average
S1	=0*1	=5*2	=14*3	=40*4	=53*5	=477/112
S2	=26*1	=45*2	=21*3	=16*4	=4*5	=263/112
S3	=0*1	=4*2	=18*3	=50*4	=38*5	=452/110
S3	=0*1	=2*2	=16*3	=46*4	=44*5	=456/108
S5	=5*1	=16*2	=31*3	=25*4	=27*5	=365/104
S6	=25*1	=46*2	=18*3	=18*4	=5*5	=268/112
S7	=13*1	=31*2	=22*3	=21*4	=25*5	=350/112
S8	=1*1	=6*2	=12*3	=43*4	=48*5	=461/110
S9	=24*1	=27*2	=25*3	=29*4	=6*5	=299/111

Table D.1: Calculations for average scores for each statement regarding the Microsoft Authenticator App.

Statements	1 Strongly disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly agree	Average
S1	=6*1	=20*2	=32*3	=44*4	=15*5	=393/117
S2	=1*1	=5*2	=14*3	=70*4	=29*5	=478/119
S3	=0*1	=0*2	=4*3	=20*4	=96*5	=572/120
S3	=2*1	=20*2	=26*3	=54*4	=18*5	=426/120
S5	=8*1	=51*2	=35*3	=22*4	=5*5	=328/121
S6	=2*1	=24*2	=35*3	=37*4	=23*5	=418/121

Table D.2: Calculations for average scores for each statement regarding the cybersecurity culture.

E Codes Generated for Qualitative Analysis

Codes	Frequency
2FA in general	42
Benefits	14
Challenges	37
Consequences	16
Customers	42
Feels unnecessary	12
Frequency of 2FA	47
Method for 2FA	47
Microsoft Authenticator App	35
Microsoft vs other solutions	23
Motimate	7
Motivation	43
Number matching	21
Qualities of employees	51
Role/position	11
Security	63
Security culture	94
Training	52
User experience	74
Workarounds	9
Work tasks	32

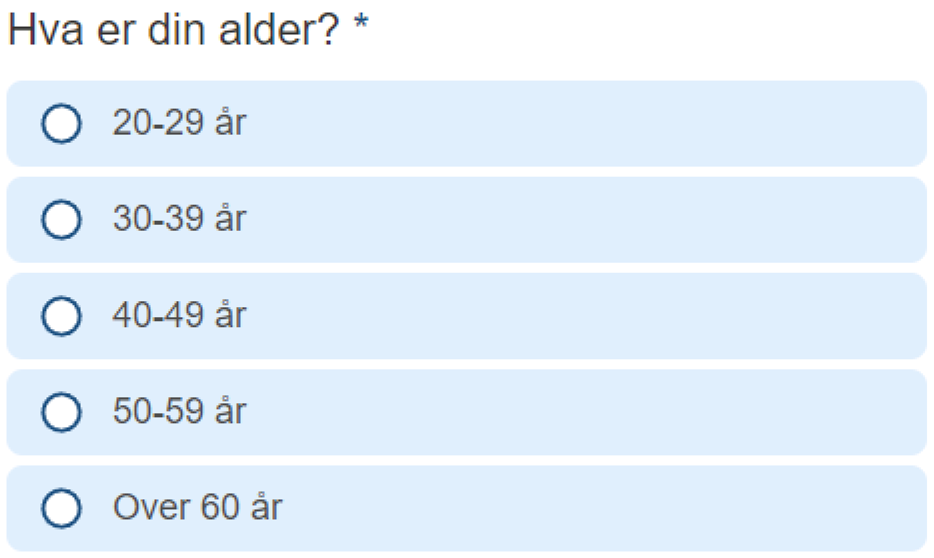
Table E.1: Codes and their frequency from analyzing the interviews.

Codes	Frequency
ADFS	1
Biometric	**2**

Compliance	2
Entrust	2
FIDO	3
Frequency	9
Google authenticator	2
Implementation	6
Microsoft applications	4
Microsoft authenticator	7
Network	2
Number matching	1
Physical token	3
Push notifications	1
Reasons for request	5
Single sign-on	2
Technical issues	8
Training	1
Uncritical thinking	3
Usability	2
User interface	1

Table E.2: Codes and their frequency from analyzing the textual answers in the survey.

F Survey Questions



Hva er din alder? *

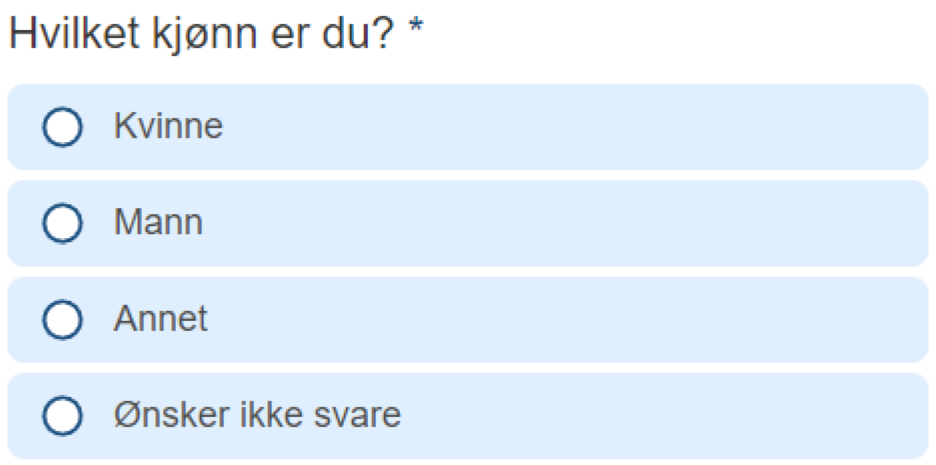
○ 20-29 år

○ 30-39 år

○ 40-49 år

○ 50-59 år

○ Over 60 år



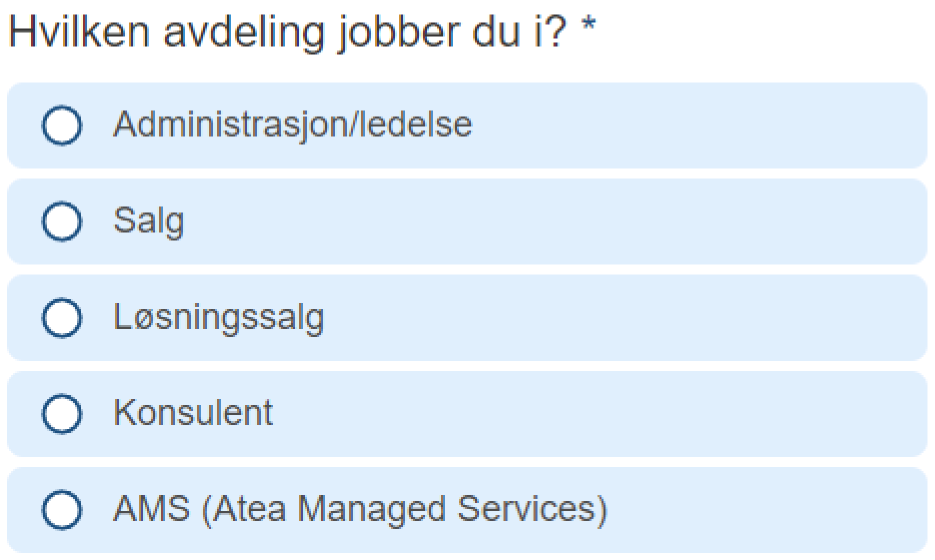
Hvilket kjønn er du? *

○ Kvinne

○ Mann

○ Annet

○ Ønsker ikke svare



Hvilken avdeling jobber du i? *

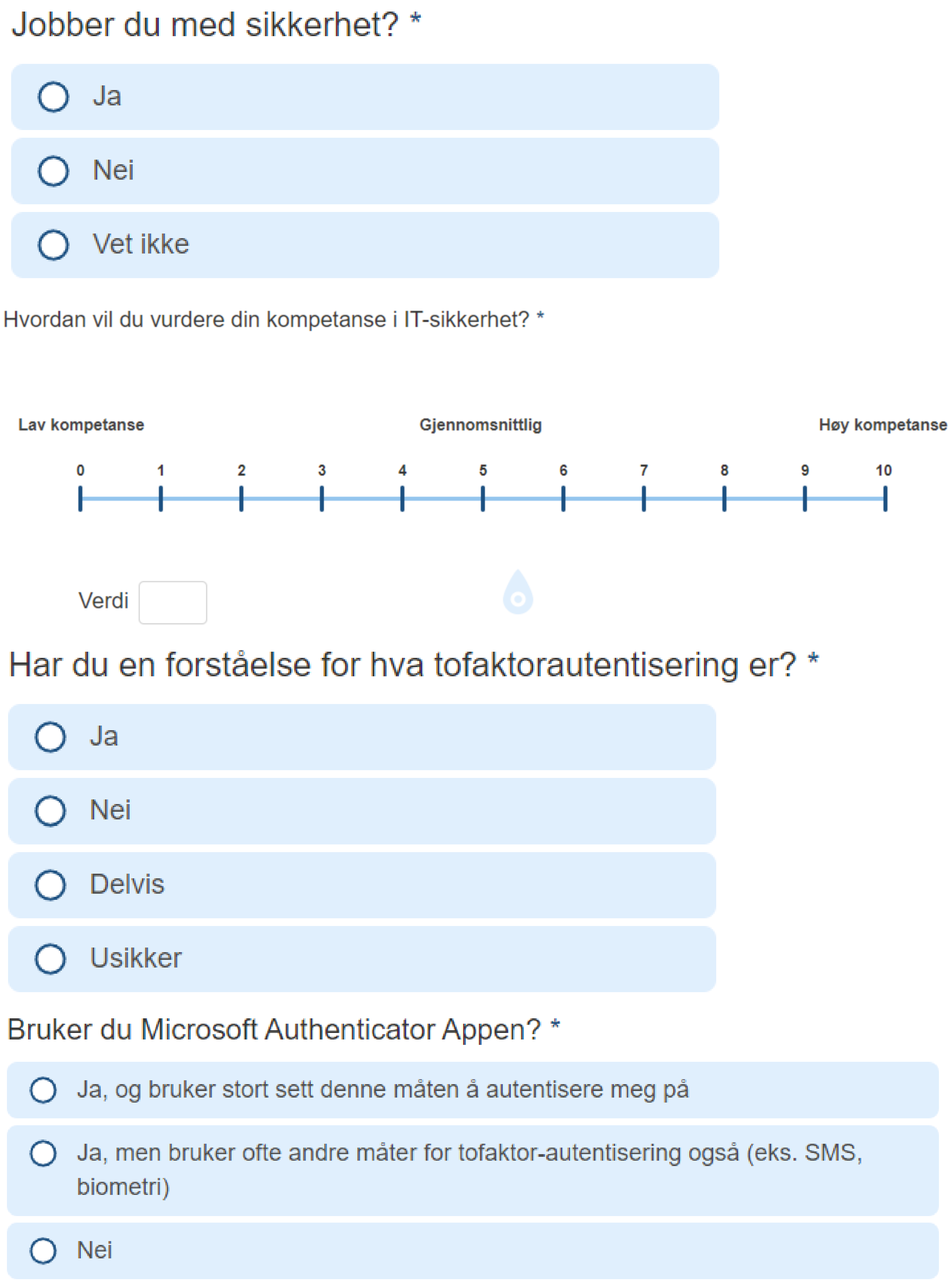
○ Administrasjon/ledelse

○ Salg

○ Løsningssalg

○ Konsulent

○ AMS (Atea Managed Services)



Jobber du med sikkerhet? *

○ Ja

○ Nei

○ Vet ikke

Hvordan vil du vurdere din kompetanse i IT-sikkerhet? *

Verdi □

Har du en forståelse for hva tofaktorautentisering er? *

○ Ja

○ Nei

○ Delvis

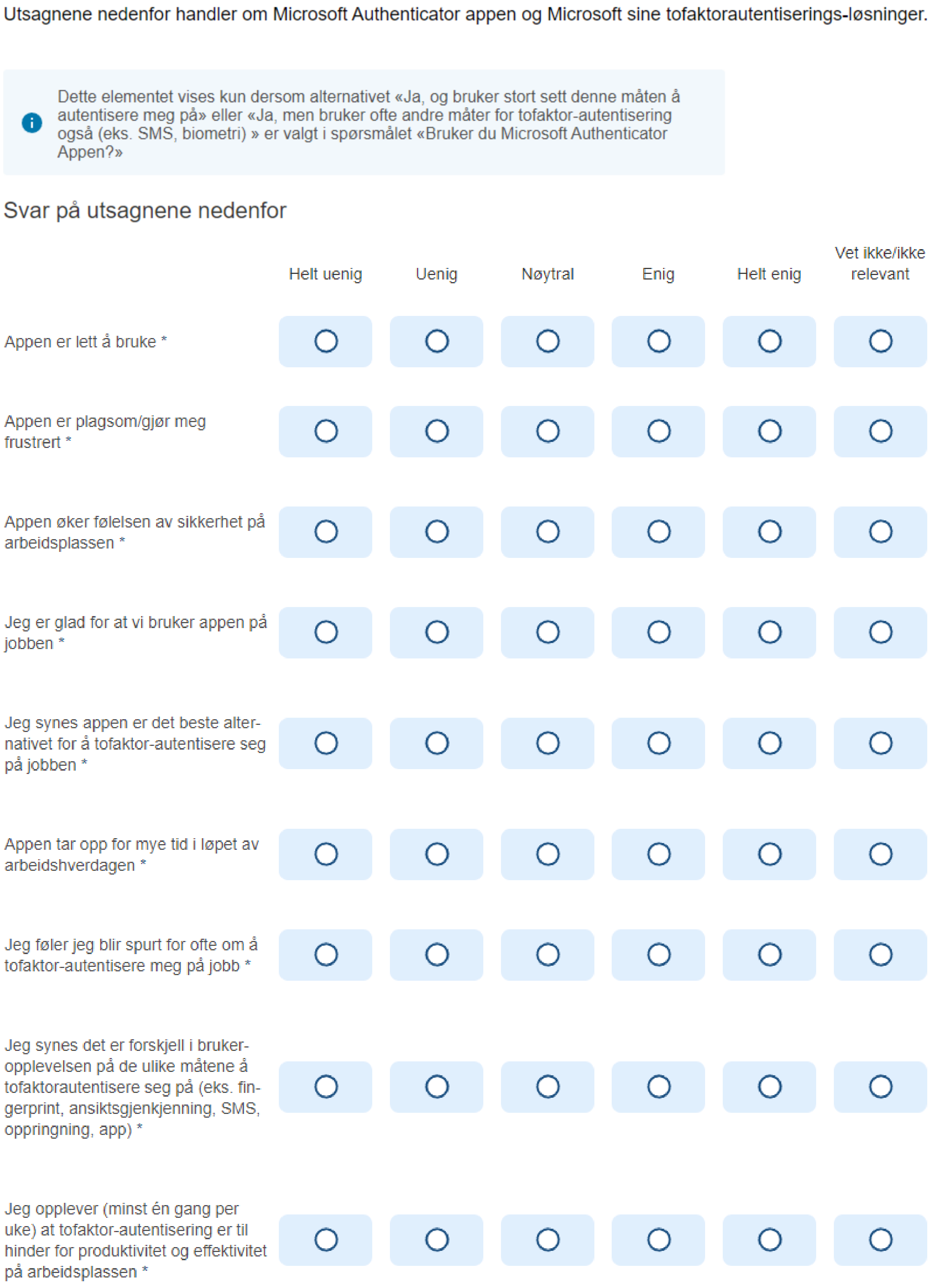
○ Usikker

Bruker du Microsoft Authenticator Appen? *

○ Ja, og bruker stort sett denne måten å autentisere meg på

○ Ja, men bruker ofte andre måter for tofaktor-autentisering også (eks. SMS, biometri)

○ Nei

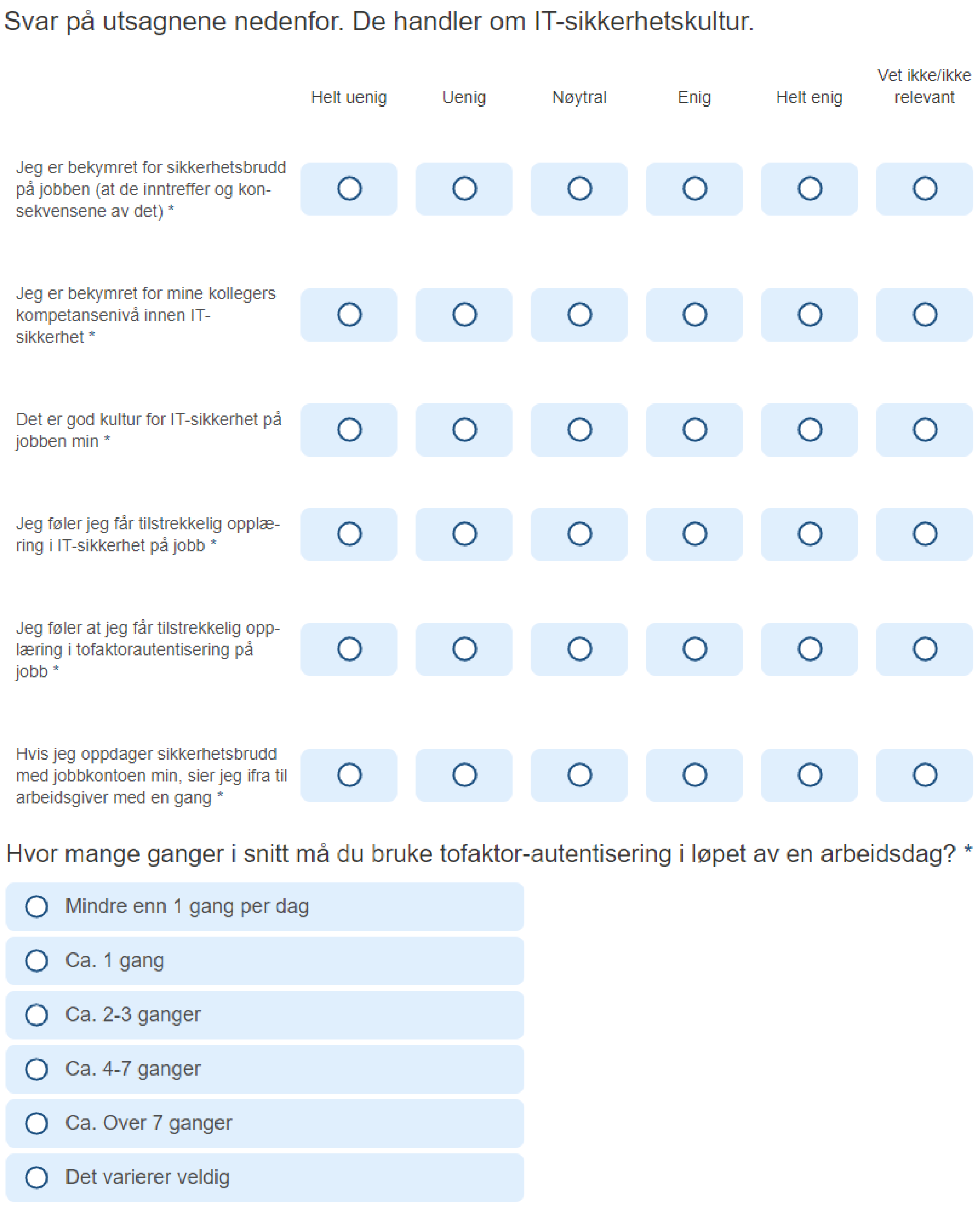


Utsagnene nedenfor handler om Microsoft Authenticator appen og Microsoft sine tofaktorautentiserings-løsninger.

Dette elementet vises kun dersom alternativet «Ja, og bruker stort sett denne måten å autentisere meg på» eller «Ja, men bruker ofte andre måter for tofaktor-autentisering også (eks. SMS, biometri) » er valgt i spørsmålet «Bruker du Microsoft Authenticator Appen?»

Svar på utsagnene nedenfor

	Helt uenig	Uenig	Nøytral	Enig	Helt enig	Vet ikke/ikke relevant
Appen er lett å bruke *	○	○	○	○	○	○
Appen er plagsom/gjør meg frustrert *	○	○	○	○	○	○
Appen øker følelsen av sikkerhet på arbeidsplassen *	○	○	○	○	○	○
Jeg er glad for at vi bruker appen på jobben *	○	○	○	○	○	○
Jeg synes appen er det beste alternativet for å tofaktor-autentisere seg på jobben *	○	○	○	○	○	○
Appen tar opp for mye tid i løpet av arbeidshverdagen *	○	○	○	○	○	○
Jeg føler jeg blir spurt for ofte om å tofaktor-autentisere meg på jobb *	○	○	○	○	○	○
Jeg synes det er forskjell i brukeropplevelsen på de ulike måtene å tofaktorautentisere seg på (eks. fingerprint, ansiktsgjenkjenning, SMS, oppringning, app) *	○	○	○	○	○	○
Jeg opplever (minst én gang per uke) at tofaktor-autentisering er til hinder for produktivitet og effektivitet på arbeidsplassen *	○	○	○	○	○	○



Svar på utsagnene nedenfor. De handler om IT-sikkerhetskultur.

	Helt uenig	Uenig	Nøytral	Enig	Helt enig	Vet ikke/ikke relevant
Jeg er bekymret for sikkerhetsbrudd på jobben (at de inntreffer og konsekvensene av det) *	○	○	○	○	○	○
Jeg er bekymret for mine kollegers kompetansenivå innen IT-sikkerhet *	○	○	○	○	○	○
Det er god kultur for IT-sikkerhet på jobben min *	○	○	○	○	○	○
Jeg føler jeg får tilstrekkelig opplæring i IT-sikkerhet på jobb *	○	○	○	○	○	○
Jeg føler at jeg får tilstrekkelig opplæring i tofaktorautentisering på jobb *	○	○	○	○	○	○
Hvis jeg oppdager sikkerhetsbrudd med jobbkontoen min, sier jeg ifra til arbeidsgiver med en gang *	○	○	○	○	○	○

Hvor mange ganger i snitt må du bruke tofaktor-autentisering i løpet av en arbeidsdag? *

○ Mindre enn 1 gang per dag

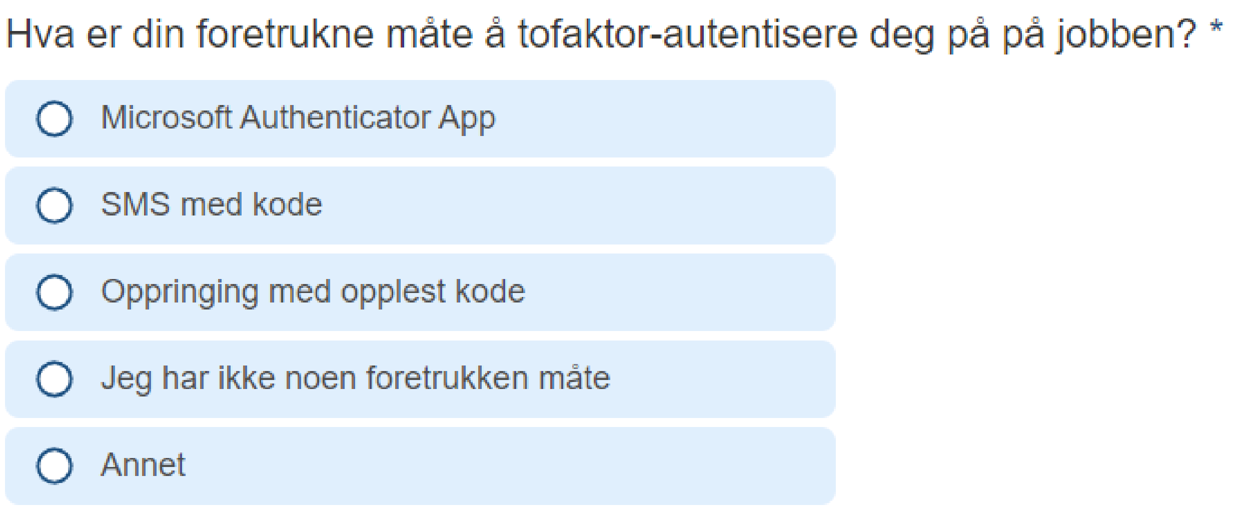
○ Ca. 1 gang

○ Ca. 2-3 ganger

○ Ca. 4-7 ganger

○ Ca. Over 7 ganger

○ Det varierer veldig



Hva er din foretrukne måte å tofaktor-autentisere deg på på jobben? *

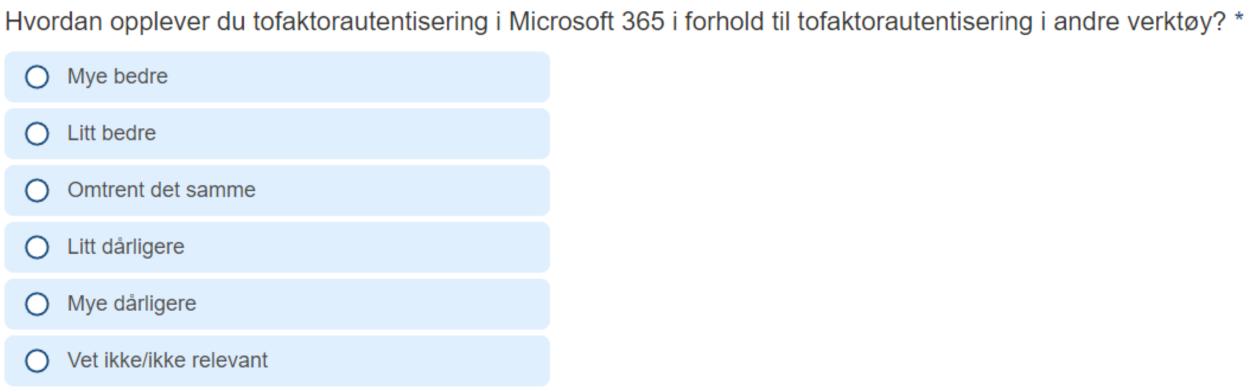
○ Microsoft Authenticator App

○ SMS med kode

○ Oppringing med opplest kode

○ Jeg har ikke noen foretrukken måte

○ Annet



Hvordan opplever du tofaktorautentisering i Microsoft 365 i forhold til tofaktorautentisering i andre verktøy? *

○ Mye bedre

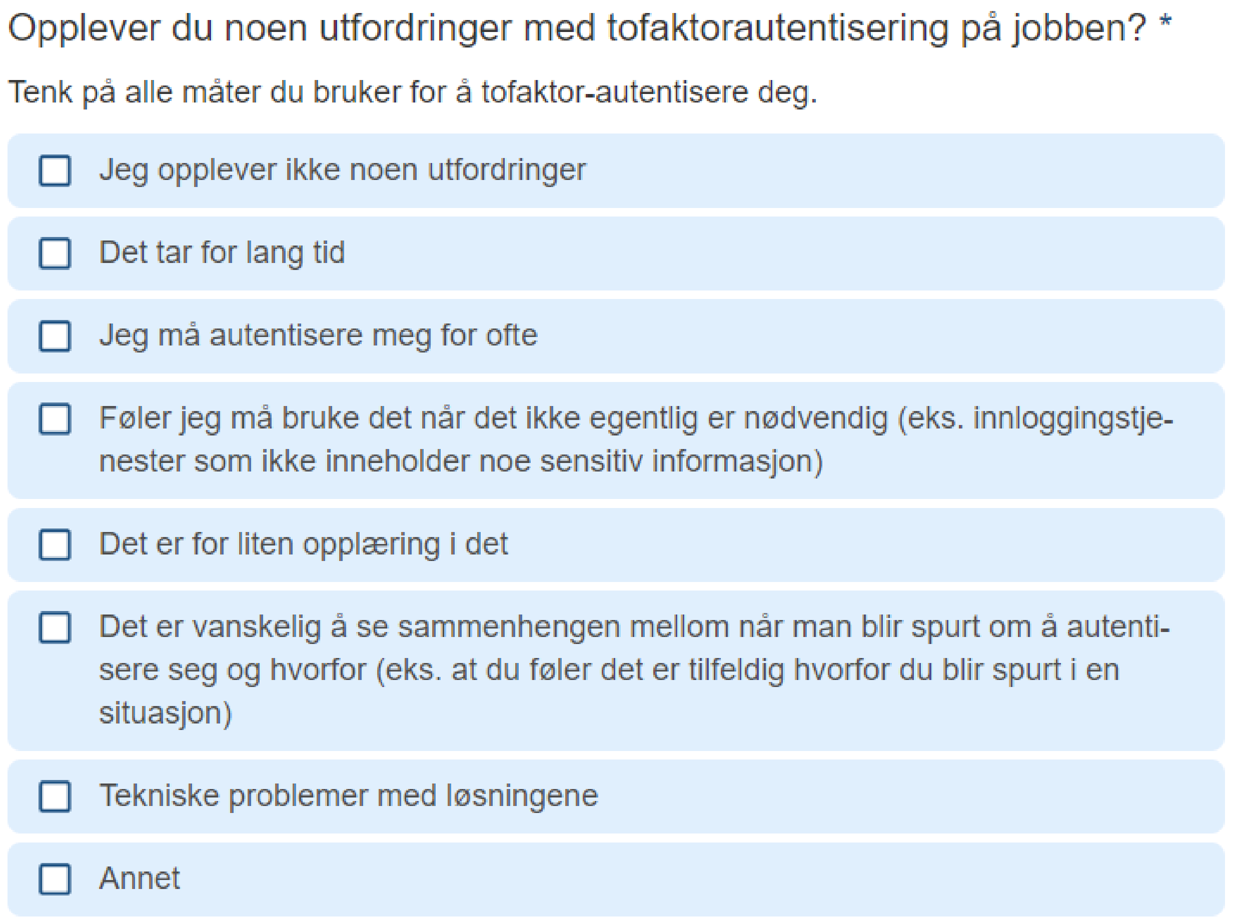
○ Litt bedre

○ Omtrent det samme

○ Litt dårligere

○ Mye dårligere

○ Vet ikke/ikke relevant



Opplever du noen utfordringer med tofaktorautentisering på jobben? *

Tenk på alle måter du bruker for å tofaktor-autentisere deg.

□ Jeg opplever ikke noen utfordringer

□ Det tar for lang tid

□ Jeg må autentisere meg for ofte

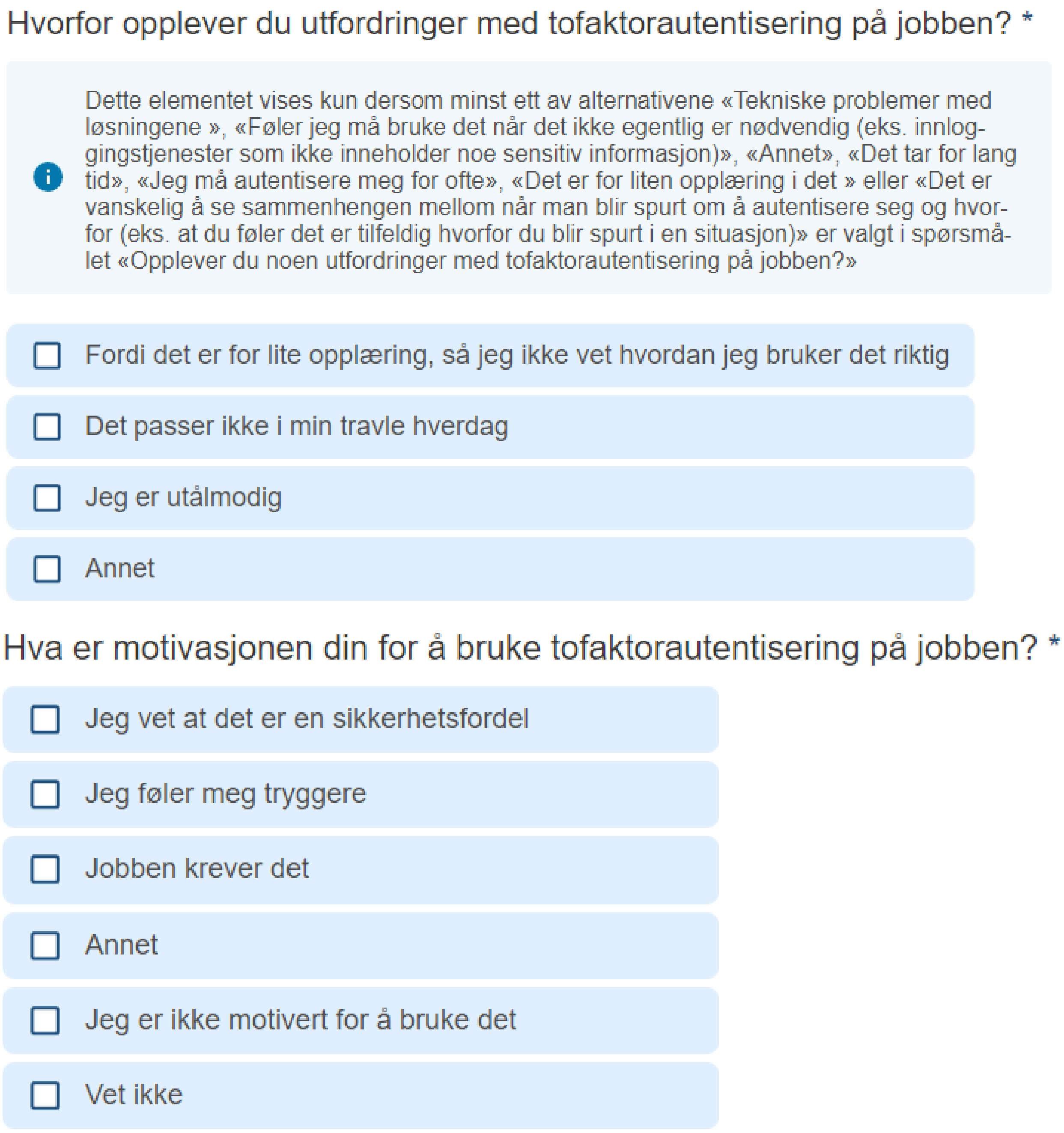
□ Føler jeg må bruke det når det ikke egentlig er nødvendig (eks. innloggingstjenester som ikke inneholder noe sensitiv informasjon)

□ Det er for liten opplæring i det

□ Det er vanskelig å se sammenhengen mellom når man blir spurt om å autentisere seg og hvorfor (eks. at du føler det er tilfeldig hvorfor du blir spurt i en situasjon)

□ Tekniske problemer med løsningene

□ Annet



Hvorfor opplever du utfordringer med tofaktorautentisering på jobben? *

Dette elementet vises kun dersom minst ett av alternativene «Tekniske problemer med løsningene », «Føler jeg må bruke det når det ikke egentlig er nødvendig (eks. innloggingstjenester som ikke inneholder noe sensitiv informasjon)», «Annet», «Det tar for lang tid», «Jeg må autentisere meg for ofte», «Det er for liten opplæring i det » eller «Det er vanskelig å se sammenhengen mellom når man blir spurt om å autentisere seg og hvorfor (eks. at du føler det er tilfeldig hvorfor du blir spurt i en situasjon)» er valgt i spørsmålet «Opplever du noen utfordringer med tofaktorautentisering på jobben?»

- □ Fordi det er for lite opplæring, så jeg ikke vet hvordan jeg bruker det riktig
- □ Det passer ikke i min travle hverdag
- □ Jeg er utålmodig
- □ Annet

Hva er motivasjonen din for å bruke tofaktorautentisering på jobben? *

- □ Jeg vet at det er en sikkerhetsfordel
- □ Jeg føler meg tryggere
- □ Jobben krever det
- □ Annet
- □ Jeg er ikke motivert for å bruke det
- □ Vet ikke

NTNU

Norwegian University of
Science and Technology