TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance

Julija Mõnnakmäe

THE ANALYSIS OF ATTITUDE AND MOTIVATION IN IMPLEMENTING AND ADOPTING NEW DIGITAL UPDATE AMONG EMPLOYEES OF TALLINN EUROPEAN SCHOOL

Master's thesis
Technology Governance & Sustainability

Supervisor: Egert Juuse, PhD

Tallinn 2023

I hereby declare that I have compiled the thesis independently
and all works, important standpoints, and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.

The document length is 11 079 words from the introduction to the end of the conclusion.

Julija Mõnnakmäe
13.05.2023

TABLE OF CONTENTS

ABSTRACT

With rapid technological developments, cybersecurity is important for organizations to discuss. However, human aspects should be observed and researched to apply digital systems and adapt them to organizations. This study aimed to identify the factors and determinants that make Tallinn European School employees (teachers and administrators) accept or reject new technological changes. The two-factor authentication system was chosen as the new technological update for TES. The Technology Acceptance Model and Unified Theory of Acceptance and Use of Technology frameworks provide an understanding of the determinants of technology acceptance. A questionnaire was used to evaluate and identify the factors that influence technology acceptance among TES employees. The results of this study show that the External factors, Perceived Usefulness and Perceived Ease of use, are the main determinants in creating attitudes, motivations, and behavior toward new technology implementation in TES. The research concludes that TES employees find the two-factor authentication system useful and are willing to try and adopt a new technological update despite differences in gender, nationality, and age.

Keywords: technology acceptance, cybersecurity, two-factor authentication, attitude and motivation

INTRODUCTION

Technology is growing and affecting nearly every aspect of society. From public to private services, digitalization has grown to simplify people's lives and work, and new system updates, digital solutions, and innovations are a part of everyday life. Even if new solutions seem helpful, not everyone is willing to try and adopt them, so technology acceptance assessment and implementation have become a vital topic to discuss (Taherdoost, 2019). Although technology usage is almost inevitable, the financial, education, military, and healthcare industries and organizations are concerned about digital safety and are becoming more vulnerable. Cybersecurity has become increasingly essential with different technological solutions and services (Ellerbeck, 2023). In Estonia, 27 115 incidents of cybercrime were reported to CERT- EE (Computer Emergency Response Team in Estonia) in 2022. The number is more extensive than in previous years and will grow. Phishing methods, service interruptions, and account takeovers caused the most significant incidents in organizations, and cybersecurity's importance in organizations have arisen. (RIA, 2023, p.11) Organizations often focus more on results and performance than on security. PwC's survey (Global Economic Crime and Fraud Survey, 2022) shows that cybercrimes are organizations' most significant fraud threats (PwC, 2022). There are multiple options for securing organizational systems that can be implemented. However, they may require more effort, financial support, and training and may not be acceptable to users.

Since the COVID-19 pandemic in 2019, the education sector has been the main target of cyber threats. Distance learning and homeschooling have opened an excellent opportunity for hackers and criminals to cause significant problems for educational institutions by accessing sensitive data and school networks. (Horowitz, 2022) Tallinn European School (TES) is part of the European school system (ES), with 26 schools under the same management. However, with the peculiarities of different countries, TES must follow regulations according to the general rules on ES. As schools are founded mainly for the European Union's employees' children, the school gathers a lot of international data and must be well secured. (Richardson et al., 2020) The TES IT policy is the schools' central policy for regulating technology and digital system usage among all employees and students, and one of the focuses of digital competence is safety. Therefore, the Tallinn

European School's digital competence, including cyber security, must continue to evolve and improve to achieve the school's predetermined goals. A new cybersecurity update will soon be launched in TES, and it is necessary to discover possible obstacles.

The study aims to investigate the attitudes and motivations of Tallinn European School (TES) employees toward implementing a new digital system. As a security measure for the system, TES intends to implement two-factor authentication for staff members (administrators, teachers who work with the school's data and have the school account provided by Tallinn European School) connected to other devices to prove the identity of the person. Since the school keeps confidential data, the school management decided to implement it to increase the system's security. The research identifies the determinants of attitudes and motivations toward the new technology. Given that research focuses on user acceptance of computer technology, the main research question is: What makes TES employees (teachers and administrators) to accept or reject the new technological change?

Sub questions:

-What are the attitudes and motivations of the employees of TES towards implementing the new digital update (two-factor authentication system)?

-How does gender, age, or nationality affect technology adaptation? Is there a difference between these variables?

Although many factors can influence the implementation of new tools such as availability of technology, design, and security, the human factor is the hardest to predict. Many models and theories have been proposed about the implementation of new technologies. However, the most widely tested and used is the Technology Acceptance Model (TAM) (Chuttur, 2009; Lai, 2017; Marangunic & Granic, 2014).

Technology acceptance model (TAM & TAM 2), and Unified Theory of Acceptance and Use of Technology (UTAUT) were chosen as the main theoretical framework models to explain and understand the user acceptance processes. The Theory of Reasoned Action (TRA) and The Theory of Planned Behavior (TPB) are the basis of the leading models and must be described to understand the main theories. While the original concept of the TAM focuses on perceived usefulness and ease of use, the UTAUT model adds determinants such as gender, experience, age, and voluntariness of use. In addition to understanding the use acceptance processes, TAM models and UTAUT provide a theoretical foundation for practical "user acceptance testing" techniques.

The TES case study used a qualitative research method to measure attitudes and motivations, although the quantitative method was also used to analyze the results of the questionnaire data. A work sample of 106 (teachers and administration team) people of different nationalities was examined to determine the attitudes and motivations for the new update among TES employees. For testing technology implementation in TES, the UTAUT theory questionnaire is used, and original questions from the theory are modified according to the example of the given thesis (two-factor authentication). The questionnaire was sent out before implementing the new update, and employees were tested immediately based on their knowledge and beliefs.

Subjective opinions based on personal and individual observer assessments of TES employees provide valuable information for testing attitudes and motivations toward two-factor authentication. The methodological limitation of this research is that the sample needs to be larger in generalizing the evaluation of motivations and attitudes in all European Schools. Despite these limitations, the data is beneficial because the attitudes and motivations have not been tested in TES before.

1. THEORETICAL FRAMEWORK

There are several behavioral and technology-related theories and adoption models proposed to describe and explain the technology acceptance and intention to use - The Theory of Diffusion of Innovations (Rogers, 1995), The Theory of Reasonable Action (Fishbein and Ajzen, 1975 & 1980), Theory of Planned Behavior (Ajzen, 1985), The Technology Acceptance Model (Davis, 1989), Technology Acceptance Model 2 (Venkatesh & Davis, 2000), Unified Theory of Acceptance and Use of Technology (Venkatesh, Morris, Davis, 2003), Technology acceptance model 3 (Venkatesh & Bala, 2008) and in addition more behavior related models, which explain the psychological part in the technology acceptance context. Studies show that TAM (1989) model's variables are still mainly used in technology acceptance research, and a significant number of models are integrated into TAM or updated by added determinants and factors to explain technology usage (Mustafa & Garcia, 2021; Marangunić & Granić, 2015; King & He, 2006).

The theoretical framework mainly focuses on two leading technology acceptance models/theories- Davis's technology acceptance model (TAM), developed in 1989, and the revised version of the same model (TAM2), created in 2000. For the empirical part of the research, the author found the most practical use of The Unified Theory of Acceptance and Use of Technology (UTAUT). UTAUT theory gathered eight behavior and technology acceptance theories, found connections between different factors, and complements TAM2 in several ways. (M. Venkatesh et al., 2003) The empirical part is conducted using the UTAUT theory since it explains the most important determinants of each theory and additional factors such as gender, age, and voluntariness. As the questions and primary theoretical points of each theory were clearly defined in UTAUT's research, UTAUT's questionnaire was used for the given thesis.

TAM and UTAUT models allow individuals to understand the cognitive processes within users and how they respond and adapt the new technologies such as objects and software and all digital-related tools and systems. Based on the appropriate theoretical framework, it is possible to investigate the intentions and attitudes of Tallinn European School employees when implementing new technology.

The Unified Theory of Acceptance and Use of Technology (UTAUT) was first proposed in 2003. The authors of the theory analyzed eight user acceptance models: The theory of Reasoned Action (TRA), the Technology Acceptance Model (TAM), the Motivational Model (MM), The Theory of Planned Behavior (TPB), Combined TAM and TPB, the Model of PC Utilization (MPCU), Innovation Diffusion Theory (IDT), Social Cognitive Theory (SCT). (Venkatesh et al., 2003) All theories were compared and explained using their main ideas in the UTAUT Model.

As the focus is on the TAM and TAM 2 models, then mostly the main concepts of these models and TPB and TRA were under observation in UTAUT. As previously mentioned, the UTAUT model was chosen for conducting the questionnaire because of added factors of gender, nationality, and age. The TAM models did not specify and focus on those factors as much as the UTAUT model, and they explained technology acceptance more broadly. Because TAM and UTAUT theories are intertwined, the author considered those models essential for the research.

1.1 Technology Acceptance Model

Davis presented the first proposed research of the technology acceptance model in 1985. He used previously developed, mostly psychology-related Fisherman's model (1967), the Theory of Reasoned Action (TRA, 1975 & 1980), and later updated by Fishbein and Ajzen the theory of Planned Behavior (1985) as his main theoretical base, which coheres with the other previous theories regarding behavior, attitude, intentions, and beliefs. (Davis, 1985) He claimed people could form cognitive opinions and attitudes before interacting with new technology. The theory fits well for the survey of the TES employee's attitudes and motivations because the research will be carried out before the actual system use.

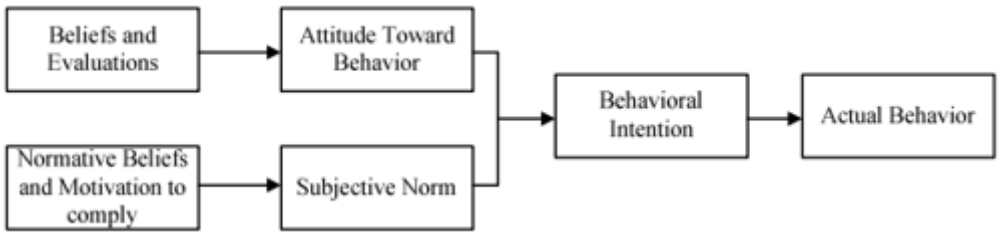
Davis investigated how the attitude and motivation toward a new system affect the use of the system. He pointed out that the most critical factors for measuring motivation and attitude are "*Perceived Usefulness*," which explains how a system simplifies the user's work and increases productivity, and "*Perceived Ease of Use,"* meaning that a person feels comfortable working without much effort. (*Ibid.*) Perceived ease of use, in turn, strongly affects perceived usefulness, and external factors, such as social influence or previous experiences, influence these two factors. If the user-friendly system increases productivity, the entire work becomes more valuable. Therefore, the relationship between perceived usefulness and ease of use is noticeable. (Davis, 1989)

Davis claimed that attitude and motivation are strongly connected to system characteristics and user behavior. He used The Theory of Reasoned Action (TRA) and the Theory of Planned Behavior (TPB) to create his theory. (Davis, 1985) The Theory of Reasoned Action and The Theory of Planned Behavior focus on people's psychological conceptions and how they form attitudes and intentions toward actual behavior. (Ajzen & Fishbein, 2000; Taylor & Todd, 1995) TRA and TPB are not explicitly created to measure behavior toward technology but to measure behavior toward whatsoever performance or acts. (Fishbein & Ajzen, 1975 & 1980) Although the theory is not explicitly created to measure technology, it is still beneficial in given research.

People would often like to separate the actual world and cyberspace. However, technology acceptance should be taken as the actual world without separation because many of our everyday doings somehow interact with technology. The illustrative example is proposed by not separating those two spaces, such as real life and life in cyberspace. For instance, employees intend to think that closing the classroom doors at TES will secure their personal belongings. However, locking computers (also an obligation by the IT policy of TES) while leaving the work desk is still an

ongoing issue because some people do not realize the need to lock their computers with their confidential data in them. Although the TRA and the TPB are not specifically created to solve digital and technological-related questions without explaining human behavior, it is tough to predict the use of the technology because the human factor plays a significant role in technology acceptance and implementation.

Figure 1. Theory of Reasoned Action (TRA)



Source: Fishbein & Ajzen, 1975, The Theory of Reasoned Action

Fishbein and Ajzen developed TRA (The Theory of Reasoned Action) in 1975 (Figure 1), which explained the relationship between beliefs, intentions, attitudes, and the endpoint of a person's behavior based on information that the person has available to them. Attitude toward the behavior and subjective norms, in turn, determine the person´s intention to perform the behavior in the future, and this intention leads to performance or nonperformance of the behavior. Beliefs can change over time, leading to an attitude and intention change and affecting a person's behavior. (Fishbein & Ajzen, 1975, p.216; Ajzen & Fishbein, 1980) We could assume that TES employees form their attitudes and motivations based on the information received from their work in TES and their personal life knowledge and experiences. They have received cybersecurity training from the TES organization, and IT policy with its cybersecurity part has been presented to each of them. However, if cybersecurity is not a person's priority in his job, then it might not occur as a salient belief. Then the attitude and intention could be negative toward the new system update.

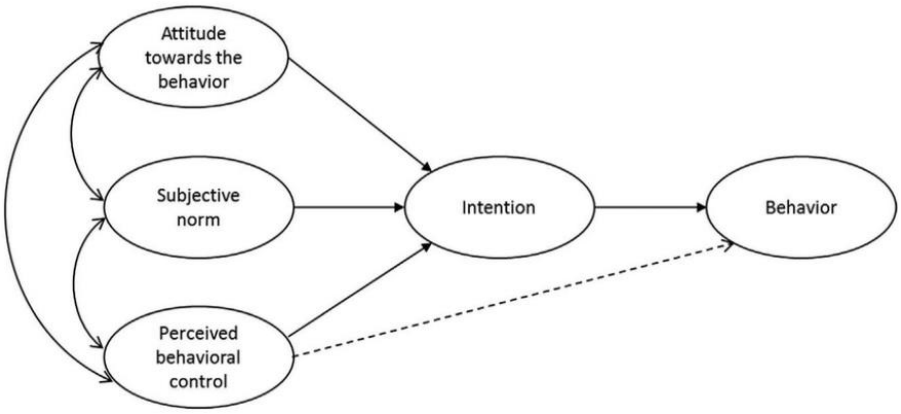
According to TRA, the behavior should be positive from the beliefs to intentions. (Ajzen & Fishbein, 1980 & 1985) In general, people intend to perform a behavior when they evaluate it positively and when close people to them think they should perform it. (Ajzen, 1985, p. 12). For example, if the person who received information about the new system believes that she/he will use it because it is helpful for him, and all the important people around also think that person should use the system, he will. The beliefs, attitudes, and intentions are positive, and a person starts to use the system. The problem occurs if the person has positive beliefs and creates a positive

attitude and intention. However, while important people do not think the system is useful - now, there is a conflict between the different factors of the behavior and the extended version. Fishbein's Theory focused mainly on beliefs or perceived consequences, and criticism of given research is that self-evaluation does not give scientific proof, even if the results explain many aspects. (*Ibid.*) The Theory of Planned behavior extends the TRA model and adds one more important determinant to explain the weak spots of the TRA model. (Ajzen & Fishbein, 2000)

To explain the TRA model from the given thesis point of view, TES employees would create their behavior based on intentions. If they believe that the 2-factor authentication can create a good, positive, and safe work environment for them, then they will be willing to try it. The more value adds to the performing behavior, a subjective norm, for example, such as people working in the same building. If the coworker recommends using the system, then TES employees' attitude might be optimistic. Also, the behavior can be positive if the more trustworthy person (TES IT- manager or Educational Technologist) encourages using the system. Although if the main goal is to have a safe environment at work, coworkers do not believe that the new system update can create that, then the intentions and attitude towards implementing the new update can change.

The Theory of Planned Behaviour (TPB, Figure 2) emphasizes the goal-directed nature of human behavior and adds "*Perceived behavioral control"* that can directly influence the behavior (Ajzen, 1991).

Figure 2. Theory of Planned Behavior (TPB)



Source: Fishbein & Ajzen, 1991, The Theory of Planned Behavior (Ajzen, 1991, p.182)

Many factors can affect intention-behavior: such as time, dominant beliefs, new information which could cause the change in intentions, confidence and commitment, individual differences, volitional control, skills, power of will, emotions, compulsions, and external factors such as time and opportunity, and dependence on others. (Ajzen, 1985) Although perceived behavioral control can directly influence the decision to perform the behavior or not, the other determinants affect behavior through the intention. When the outcome and prediction are equal, then we speak about TRA, although when the prediction of behavior failed by external factors, we speak about TPB. (Ajzen, 1985; Pavlou & Fygenson, 2006)

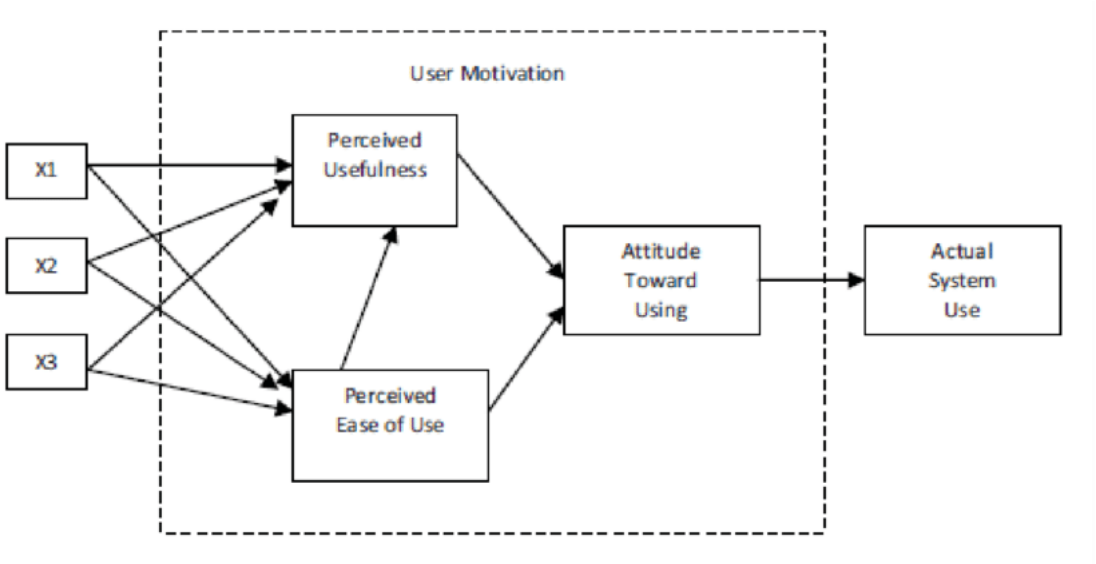
To try to explain this theory with an example of given research, using a two-factor authentication method would be the actual performance of the behavior. To use it or not, the intention must be primarily positive. For example, colleagues suggest using it, or people believe that it helps them to be safe in the digital environment. When all previous determinants are equal (equally positive or negative), the final stage of the behavior will be formulated by the previous factors. When a person believes that he will use the system (this is his final behavior), although he does not know how to do it, this qualifies for perceived behavior control, which directly affects the behavior. However, all other determinants may not be equal.

Davis focused on how motivational variables and developed measures of these variables influence system features. (Davis, 1985) His research aimed to develop a model for user acceptance testing in information systems. Davis's proposed model (Figure 3) explains user motivation in general, where attitude plays an important role in actual system use. In turn, attitudes are influenced by two of the major factors in the TAM model:

1. Perceived Usefulness- "*Perceived usefulness is defined as the degree to which an individual believes that using a particular system would enhance his or her job performance.*" (Davis, 1985, p. 82).

2. Perceived Ease of Use- *"Perceived ease of use is defined as the degree to which an individual believes that using a particular system would be free of physical and mental effort"* (*Ibid.,* 82).

Figure 3. Technology Acceptance Model (1986)



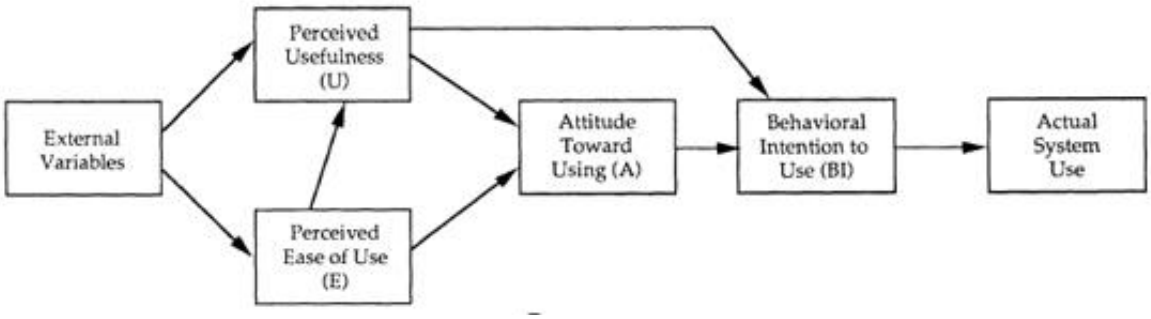
Source: Davis (1985, p.24) Technology Acceptance Model

Davis (1985) developed 14 questions for the survey to evaluate the system's Perceived Usefulness and Ease of Use. He asked specialists to conduct the statements and to create a valuable survey, and the same statements are used to determine the attitudes towards the new system update in TES. Davis argued that before implementing the new technological system or tool, the organization should be aware of the needs of employees in their jobs. Perceived Usefulness is the priority in new system implementation. In the case of this study, the new system update secures the needs of the organization in general. However, it is difficult for TES employees immediately to find the Perceived usefulness in their job because the new system update does not, for instance, help them

to solve their issues more quickly as in Davis's research, where employees found e-mails more beneficial than handwritten mail. The new system update in TES requires even more time. However, if it can protect from data leaks and the system can minimize human errors, then the goals are achieved. The organization focuses on perceived usefulness, although it might differ for TES employees individually. Therefore, the study aims to determine what is more important for TES employees, The perceived usefulness, or the ease of use. By Davis, the priorities must be placed on the employees and their job and tasks rather than technology (Davis, 1985, p.218).

Created in 1989, the TAM model added Behavioral Intention (Figure 4), which was not the focus of the TAM (*Ibid.*) prior model. According to the TAM model, perceived usefulness directly influences behavior Intention. Perceived usefulness can directly influence behavior intention, although it can also be influenced through attitude. (Davis et al., 1989) The goal of the TAM is to focus on the relationship between Attitude, Perceived Usefulness, Perceived Ease of Use, and Behavior Intention to explain user acceptance, which were the main parts of the first TAM version as well. In both TAM models, Usefulness and ease of use are the main determinants of user acceptance.

Figure 4. Technology Acceptance Model (TAM)



Source: Technology acceptance model TAM (Davis et al., 1989, p. 985)

Two-factor authentication is relatively easy to use in the system design. TES employees know how to log in to Microsoft 365 accounts successfully and they had the same training and policies on using the work accounts. The new system requires logging in the same manner as before, but two additional steps have been added to the previous system, which only requires a small amount of extra time. Because of the added extra steps to logging in, TES employees could find the new system uncomfortable. Their experiences and attitude toward the system could primarily be also negative, which can create a negative behavior intention to use. Even if TES employees find the

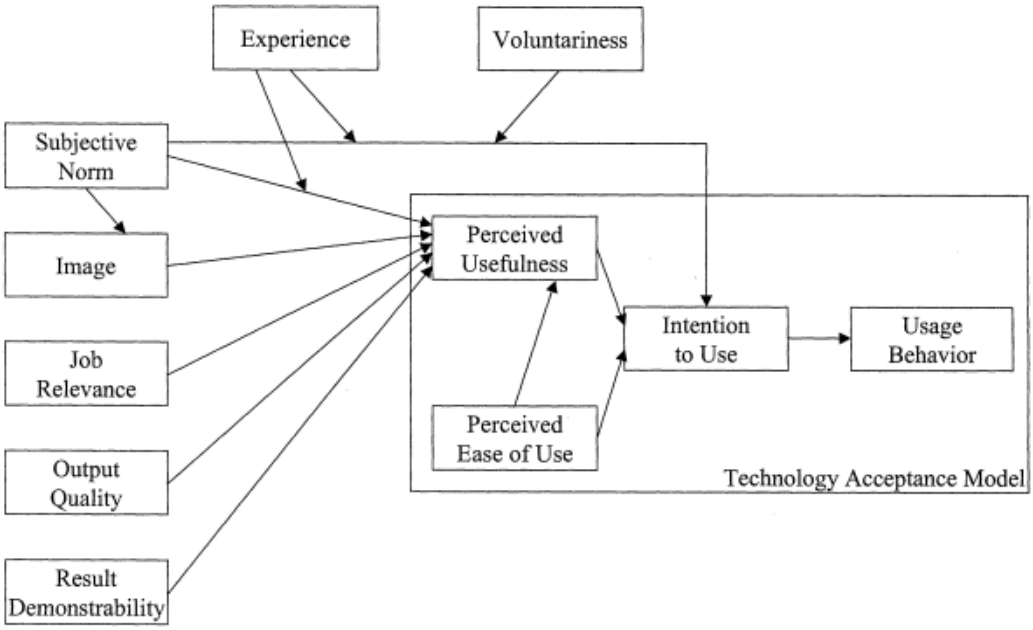
system is easy to use, the external variable, such as previous experience, can also influence their usefulness and behavior.

Both TRA and TAM point out that relevant beliefs create attitudes. The difference is that TRA researchers claim that beliefs appear for each new object/subject/system, and TAM focuses on technology acceptance in general by two determinants: Usefulness and Ease of Use (Davis et al., 1989, p. 988), where the expected outcome of the Usefulness and Ease of Use is mostly positive.

Extended Technology Acceptance Model (TAM2)

In 2000 Venkatesh and Davis proposed new extensions to a TAM model and named it TAM 2 (Figure 5). They kept the most important determinants as a core for user behavior from the TAM 1 model: Perceived Usefulness and Perceived Ease of Use, Intention to Use, and added more specific elements to the model. TAM 2 explains external variables more than in the previous TAM model.

Figure 5. Technology Acceptance Model 2



Source: Technology Acceptance Model 2 (Venkatesh & Davis, 2000)

Social influences, such as Experience, Subjective norm, Voluntariness, Image, and cognitive instrumental processes, such as Job relevance, Output quality, and Result demonstrability, were

added to the TAM2 model. TAM2 explains that *subjective norms* on the intention to use above perceived usefulness can occur when users are mandated to use the system, not voluntarily. (Venkatesh & Davis, 2000) In the case of our study the new system update will be mandatory implementation for TES employees.

The image represents social influence, a preference group membership, which determines the individual's social status. (*Ibid.*) As the research sample is teachers and staff members, the preference group membership could play some role in user intention depending on the job position.

Job relevance is an essential component in usage behavior. It judges whether the system adoption is relevant to his/her job. It has a direct influence on perceived usefulness. (*Ibid*.) In this case, TES employees must evaluate cybersecurity's importance as perceived usefulness.

Output quality determines how well the new system will perform its functions and whether the output quality satisfies job goals and needs. (*Ibid.*) Employees will be questioned before the actual system use. Quality input cannot be assessed in the given research but could be measured in further studies after implementing the 2FA system in TES. *Result Demonstrability* is defined by Moore and Benbasat (1991, p.203) as the "*tangibility of the results of using the innovation"* (Venkatesh & Davis, 2000, p.192) and also occurs after the testing of the new system.

Experience determines previous interaction with the system and can influence the perceived usefulness or directly the intention. (*Ibid.)* Suppose some TES employees had previous experience with the same or similar 2-factor authentication system. In that case, it can affect their attitude and motivation toward using the same system in their work.

The explanation by TAM 2 is that subjective norms create the intentions before the system is applied. Nevertheless, after implementing the system, individuals can directly test it and change their opinions. Direct system use and experience can overcome the first fear of using the system and increase the system's productivity. If TES employees do not like the system, their opinion could change after testing it. Over time it can also change the attitude toward the system. (Venkatesh & Davis, 2000, p. 190)

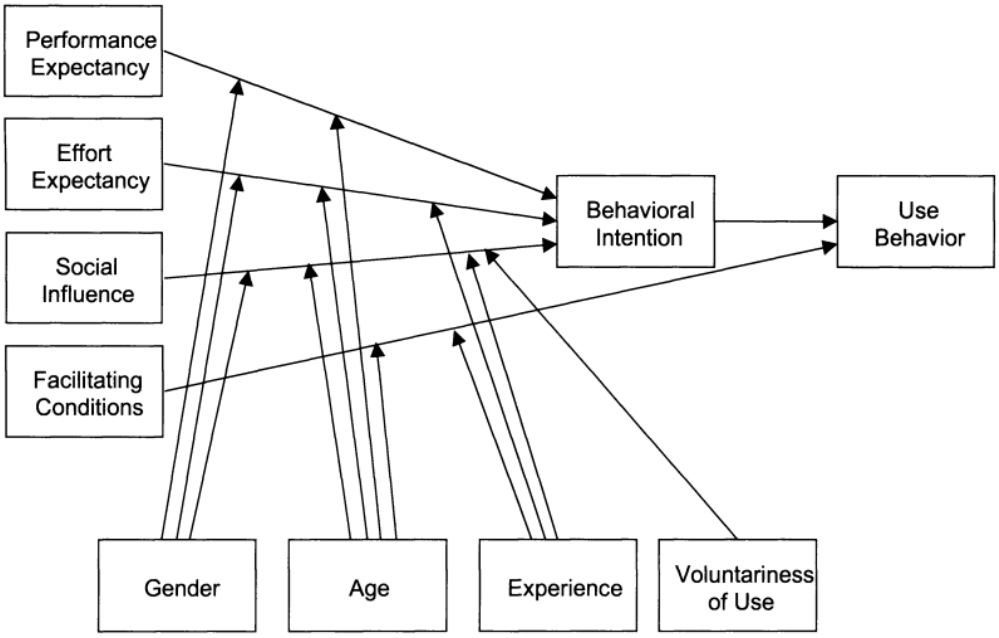
The model shows that all external variables are mainly connected to perceived usefulness, which creates the intention to use or not to use the system and leads to the usage behavior. When all these modifiers are equal, the system is easy to use, employees understand why it is necessary, the employee's interests and the organization's interests are compatible, and everyone thinks that

everybody in the organization benefits from the new system update, then intentions, attitudes, and motivations are positive, and the system will be in use.

TAM models are a prominent framework for testing the attitudes and motivations toward the technology. However, TAM and TAM 2 models did not address age and gender or how these variables could influence technology acceptance. Therefore, the Unified Theory of Acceptance and Use of Technology was chosen to add more value to the given research, find out if those variables somehow correlate, and investigate whether any similarities or differences between age and gender emerge in technology acceptance research.

1.2 A Unified Theory of Acceptance and Use of Technology (UTAUT)

Figure 6. A Unified Theory of Acceptance and Use of Technology



Source: UTAUT (M.Venkatesh et al., 2003, 447)

According to the new model (Figure 6), the main variables influencing use behavior intention were performance expectancy, effort expectancy, and social influence. Gender, age, experience, and voluntariness appear to be moderating variables in the UTAUT model, they indirectly influence intention behavior by showing how these factors affect four main determinants: Performance expectancy, Effort expectancy, Social influence, and Facilitating conditions. Performance expectancy brings together several factors reflecting the perceived usefulness (from TAM and TAM2 models). According to Venkatesh's research, performance expectancy is still the most vital determinant of behavior intention in mandatory and voluntary settings. (Venkatesh, 2003 p. 447)

Although there is a finding that gender and age are also part of behavioral intention, they are not direct predictors of behavior. The theory claims that it tends to be more task-oriented and aims to make the behavior of the results more salient. Gender schema theory adds that age and socialization are crucial in predicting behavioral intention. Gender differences have appeared in technology acceptance theories analyzed by Morris and Venkatesh (M. A. Morris & Venkatesh, 2000; M. G. Morris et al., 2005). The findings show that men were more related to Perceived Usefulness and women to Perceived Ease of Use.

Effort expectancy formulates behavior intention based on the use of the system. According to TAM and TAM2, models' Effort expectancy would reflect Perceived ease of use. Although studies show that perceived ease of use depends on whether the behavior intention is tested before or after implementation. Venkatesh and Morris claim that women are affected by effort experience more than men, especially younger women who do not have previous experience with the new system (M. Venkatesh et al., 2003).

Social influence is the determinant that depends on the close people's opinions towards the system according to TAM and TAM 2 models. In UTAUT theory, social influence has a bigger concept, where social status appears to have significant influence, and the potential user feels the social pressure. The feeling of reliance on others occurs more in the case of mandatory system use (early stages). (*Ibid.)* In technology acceptance, women are more likely to listen to others' opinions in implementing a new system in forming the intention. (Venkatesh et al., 2000) Therefore, social influence is a salient determinant among women more than men. Affiliation as a part of the social influence can change with experience and age (Venkatesh & Davis, 2000; Venkatesh et al., 2003). More likely that older people's need for affiliation is more salient and can change with experience. (Venkatesh & Davis, 2000). Older women, especially in mandatory settings, tend to be more strongly influenced early in developing behavior intentions than older men. (Venkatesh et al., 2003)

Facilitating conditions are the state where the organization provides all required devices, training, help, and guidance in using the new technology or updates. The person feels like they receive all the needed support from the organization in using the new technological updates or systems. (*Ibid.,* 453). Three main characteristics of that determinant are perceived behavior control, facilitating conditions, and compatibility. According to Venkatesh's research (2003), facilitating conditions influence user behavior but not behavior intention. The effect of the given determinant increases when people start to use the new system. Venkatesh (2003) studies show that older people are more in need of help and assistance at jobs and more willing to ask for help from system support. In the case of the study, TES has an IT- team with the IT manager and educational technologist who support the employees in all digitalization and technology-related questions.

Although two determinants, anxiety, and self-efficacy, were discussed in the other studies and considered to be added to the UTAUT model, Venkatesh found that perceived ease of use can drive them. However, they will not significantly influence behavior intention, and those factors are not in the research's focus. *Attitude* toward using technology is defined as an "*individual's overall*

affective reaction to using a system" (M. Venkatesh et al., 2003, p.455). In the previously explained models, Attitude was an independent determinant of user behavior. The given model explains it as part of the effort expectancy but not significantly influencing behavior intention. (*Ibid*.)

All the theories described and explained in this study were extended and researched by the same authors in different years, so the concepts of TAM models and UTAUT integrate. However, the research aims to determine what influences TES employees' attitudes and motivations. The author wants to use the international TES sample to find any connections between age, gender, nationality, and employees' attitudes and motivations.

1.3 Criticism of TAM and UTAUT

Although TAM is one of the most well-known technology acceptance theories in user technology acceptance research, it has its concerns. The TAM and UTAUT models are criticized because of their simplicity. (Shachak et al., 2019) As previous chapters explained, the most important determinants of technology acceptance in people´s behaviors are perceived usefulness, ease of use, and intentions. Then academics argue that explaining and generalizing technology acceptance is too simple based on the presented factors in TAM and UTAUT, and the reality is more complex than just in those main determinants. (Hirschheim, 2007) More individual- based differences and people´s abilities should be considered, and more modifiers should be added to both models. (Kim et al., 2008; Straub, 2009, p. 638-640) Nevertheless, despite the critique, the presented models in the research are the most used theories in technology adoption studies and testing. The statements found in UTAUT Venkatesh's research were made long ago, considering that the theory was proposed in 2003. From 2003 to 2023, technology growth has been significant, and findings regarding gender and age might be different now. A study among employees of the Tallinn European School will be conducted based on the previously discussed theoretical background.

2. EMPIRICAL PART

Studies have shown that the weakest link in creating a secure system and investing in technological cybersecurity solutions is technology user and human contact (RIA, 2023; Jeong et al., 2019). This leads us to the central question of the research: why are people willing or refusing to adopt new digital systems, what is their attitude and motivation toward the new digital updates. Weak and reused passwords are an organization's weak spots and give attackers access to submitting crimes in organizations, so the two-factor authentication system is one of the tools to prevent the system from threats. (RIA, 2022)

Security depends also on usability. Effective security generally renders usability both difficult and complex. (Dhillon et al., 2016) Achieving effective security and usability simultaneously is challenging because systems and data processing are more complex now. Based on the previously discussed theory and models, the author classifies Security as Perceived Usefulness, and Usability as Perceived Ease of Use. If people find it useful, they will probably use technology related to security, even if it requires more effort. If they do not prioritize cybersecurity in their life, they will likely not have a good attitude and motivation to use new systems related to security. (Magalhaes, 2018) The implementation of cybersecurity measures depends on how people value it.

This chapter provides an overview of the importance of cybersecurity in Tallinn European School, its policies, and the importance of cybersecurity in the European Schools system. The chapter explains the survey process and its outcomes. The empirical part of the research concludes by analyzing the gathered data and findings.

2.2 The importance of cybersecurity

Attackers and organized crime groups are becoming more experienced in finding solutions to get inside the systems and technologies that organizations rely on. Half of the global organizations have experienced cybercrime or threats. (PwC, 2022) By the report of the World Economic Forum in 2022, 95% of cybersecurity breaches are caused by human mistakes (World Economic Forum, 2022; The Hacker News, 2021). Recent discussions have focused on security versus usability, and more complex systems must be protected. However, the reality is the opposite: the more we use different systems, the more insecure they become because people's understanding of cybersecurity depends on different aspects: design, policies, human mechanisms, knowledge, and the safety of the systems. If one of these aspects is not addressed, the security system fails. (Yee, 2004)

To prevent crimes, organizations must evaluate the organization's weak spots and identify where hackers and criminals can potentially enter the system and carry out attacks. The first step in improving cybersecurity in organization and preventing crime is to educate employees and create a *"cybersecurity*" culture in the organization, starting with simple things, such as creating a safe password and locking the computer at work. The next step would be to use anti-fraud technology in the organization and keep control of the data processed (Ellerbeck, 2023). A password is one of the most accessible options that does not require complicated training and ensures the first step to safety. There have been many recommendations for creating secure passwords, however people still use passwords that are simple to guess.

The Microsoft identity security director, Alex Weinert, protects Microsoft accounts and recommends adding a two-factor or multifactor authentication system to job accounts to secure the organization. He states that one of the issues is the very easily guessed passwords (weak passwords), which are also the default passwords, most often used more than once in different accounts. Also, poor password policies create issues in the cybersecurity of organizations. (Weinert, 2023; Aloul et al., 2009) Stolen or weak passwords accounted for 81% of hacking breaches. There were 1.65 billion attack-driven signals detected in January, 2020 (Weinert, 2023; Use Stronger Security Than Passwords Alone, n.d.) and three main causes of attack are breach replay, password spray, and phishing. Microsoft researched passwords and discovered that over the past 30 years patterns repeat themselves. Even when organizations require systematic password changes over time, people choose to keep their passwords mostly the same. (*Use Stronger Security*

Than Passwords Alone, n.d.) Therefore, it is not difficult for cybercriminals to predict passwords, even if they occasionally change.

Authentication systems effectively protect against cyberattacks (Weinert 2023; Aloul et al. 2009). In particular, password spray attacks, such as brute-force attacks, occur when the criminal uses the same password against many employees and tries to find accounts that match the same password. The reuse of passwords is a widespread type of cyber-attack, that causes a lot of issues in organizations. (Weinert, 2023) One of the prior recommendations for organizations is to create a strong password policy for employees (Jones, 2023) which has been achieved in TES. IT-policy has recently been updated.

National Institute of Standards and Technology, U.S. The Federal Agency (Grassi et al., 2017) has proposed digital identity guidelines (Hicock, 2018) for users and identity administration. Since TES uses Microsoft accounts, the password policy recommendations for Microsoft 365 accounts (Kwekuako, 2023), provided by Microsoft's security team are beneficial in policy design for TES, Password management is described in TES IT policy in Chapter 5.3. This highlights the requirements for creating a password in TES. There is no added rule for two-factor authentication because the new system still needs to be implemented officially.

2.2.1 Two-factor authentication (2FA)

Microsoft defines 2-factor authentication:
„Two-factor authentication (2FA) is an identity and access management security method that requires two forms of identification to access resources and data. 2FA gives businesses the ability to monitor and help safeguard their most vulnerable information and networks.“ (Microsoft, 2023)

There are different options for a 2FA to identify a person, although the research focuses on the SMS verification system. SMS or text messaging can be used for two-factor authentication when a message (text or number) is sent to a trusted phone. The user is prompted to interact with the text or use a one-time code to verify their identity on a site or app.

In the example of TES, logging into the Microsoft 365 account, the system immediately sends the message (to the person´s phone number). Employees are prompted to use a one-time code to verify their identity on a site or app. The frequency at which the 2FA prompts users depends on the organization's setting. Most likely, the system asks for identity confirmation when people sign in from a different device or change their location or password. Therefore, there is no need to verify their account each time they log in. (Microsoft, 2023) Two-factor authentication is more secure than simply inserting the password, and to adopt a more secure system, only a trustful mobile device is required.

2.3 Introduction of Tallinn European School

To understand each part of the research, it is essential to provide an overview of the organization under investigation and why that school is the case of analysis. Tallinn European School (TES) is an accredited European school in Tallinn, Estonia, with approximately 500 international students (51 nationalities) and 120 staff members. The Ministry of Education and Research established the TES in 2013, and the school has grown every year. (TES, 2023) The mission of the school is: *"To provide a broad, balanced, creative, multicultural, and multilingual education in a highly motivating learning environment to prepare the future citizens of an ever-changing world."* (Tallinn European School, 2023)

The owner of the TES is the European School Foundation (Sihtasutus Euroopa Kool) founded by the Estonian Government. The Council of the Foundation includes members of several institutions: the Ministry of Education and Research, Ministry of Economic Affairs and Communications, Ministry of Finance, Education Department of Tallinn, and EU-LISA. (TES, 2023; Office of the Secretary-General of the European Schools, 2023) TES is part of the European school system within 26 European Schools in 15 EU countries. 21 out of 26 schools are accredited, meaning they offer a European curriculum and a European Baccalaureate. Pedagogical expectations for European schools are integrated into the educational framework of member states, although they follow the European School's curriculum. (TES, 2023) Therefore, TES must operate and observe the Estonian Ministry of Education rules, being simultaneously part of the European Schools system.

The Estonian Ministry of Education and Research developed Education Strategy 2021-2035 (based on European Union reguations), which sets the goals for Estonian education and digital competencies, including cybersecurity aspects. The same goals apply to the TES (Ministry of Education and Research, 2021). The central managing organ of European Schools is the Office of the Secretary-General, which supervises and advises in all areas of the schools: financial, administrative, legal, and pedagogical. The Office of the Secretary-General of European Schools comprises the EU Commission and the Ministers of Education of each EU member state. (Office of the Secretary-General of the European Schools, 2023) The school provides high academic results (OECD, 2022) by having highly profiled teachers and support staff (medical support, support teachers, nurses, psychologists, and anti-bullying teams). Every year, the number of students, staff members, and services increases, making it more important to have a safe digital

environment at school. In addition, to expect the TES to be digitally competent and innovative, the author must explain the school's main objectives. The Pedagogical Unit of the Office of the Secretary-General has developed eight key competencies for Lifelong Learning in European schools, and one of the main competencies is the digital competence of European schools where digital competence is defined as:

"Digital competence involves the confident, critical, and responsive use of, and engagement with, digital technologies for learning, work, and participation in society. It includes information and data literacy, communication and collaboration, digital content creation (including programming), safety, (including digital well-being and competencies relating to cyber security), and problem-solving." (Office of the Secretary-General [Pedagogical Development Unit], 2018, p.29)

Following the given framework for the digital competence of the school, where digital competence is described as being innovative, digital, and technology related in all areas of the school while being responsible for safely using the technologies. Testing employees' attitudes and motivations of TES toward a two-factor authentication system is helpful and valuable for TES and the European school community. To prevent misunderstandings and crime while dealing with digital systems and technological devices, TES implemented an IT policy for all employees. The document must consist of the aims and goals of European school guidelines and be created according to European Commission rules on IT at European Schools. The document was updated and approved by the board in 2022. To prevent cybercrime in TES, the IT Policy has the part of cyber hygiene and other simple and vital steps required to keep school safe. The IT Policy (2023) of TES includes the following (Tallinn European School, 2022):

- The Rules of Procedures for the Use of Information and Communication Technologies of Tallinn European School (Staff)
- The Rules of Procedures for the Use of Information and Communication Technologies of Tallinn European School (Pupils)
- The TES Microsoft Teams Netiquette
- The Bring Your Own Device (BYOD) Policy
  The official guidelines for choosing a mobile device related to the BYOD Project (*Ibid*.)

The policy covers different aspects of the school, from students bringing their digital devices to cybersecurity (how to create passwords, what system the school uses, how the accounts are created,

how to lock the computer, data processing, etc.). In addition, the policy explains how to deal with incidents and who is responsible for what while using the school's information technology. (TES, 2023) Even with IT-Policy in TES, in everyday work, TES still faces difficulties among employees, where the rules still need to be followed 100%, so with the help of technology is possible to prevent the incidents that data leaks and crime could cause. Two-factor authentication has not yet been added to the IT-Policy policy. If the research outcome is positive for the organization, then the requirement for two-factor authentication will be added to the school's policy.

2.4 Methodology

Participants

A work sample of 106 (teachers and administration team) is examined to determine the attitudes and motivations for the new update among TES employees. Since the new system update concerns all employees with school Microsoft 365 accounts (educators and administration team), the sample was chosen based on that. All participants work in the same organization and must follow the policies and regulations of TES.

The Questionnaire

For testing technology implementation in TES, the UTAUT theory questionnaire is used, and original questions from the theory are modified according to the example of the given thesis (two-factor authentication). The questionnaire consists of 16 questions on a Likert 5-point scale (from strongly disagree to strongly agree). Demographic and open-ended questions were added to provide more input to the research, given that the research is testing motivation before the actual system is used.

The UTAUT theory's questionnaire was based on eight different acceptance theories, although in questioning TES employees, the author mainly used questions related to TAM, TAM 2, TRA and TPB models. The first three questions collect demographic data- gender, age, and nationality. General cybersecurity questions are followed, and the central part of technology acceptance testing is divided into five sections: Performance Expectancy (Usefulness), Effort Expectancy (Use of the system), Social Influence, Facilitating conditions, and Attitude toward using technology. Data was analyzed in Excel and Microsoft Forms. Both qualitative and quantitative methods were used to analyze the data, and cross-tabulation was used to analyze the findings related to gender and nationality.

Procedure

A questionnaire, conducted in Office Forms, was sent out to test attitudes and motivations toward two-factor authentication system among Tallinn European School employees before implementing the new system. The questionnaire was handed in with a short description of the two-factor authentication, and how people should use it in TES was explained. The survey was sent without the IT- team's initial introduction to avoid creating a bias based on the presentation of the IT- team. The questionnaire was open for one week, although the time limit was not announced because people were encouraged to complete the survey as soon as possible to get an immediate reaction. The researcher promised the participants that the survey would be anonymous and used only for the study. The reminders were sent out to all schools' communication platforms every day during the week, also reminded during the staff meetings and in the school’s newsletter (only for teachers and adminstration team) and the response rate (63%, 67 respondents) is lower than expected.

2.5 Data analysis

Sixty-seven people aged 25-65, participated in the questionnaire and almost half of the participants were in the age group–30-39 years old. The majority of participants were women (49 out of 67). Twenty-one nationalities were presented, and most participants identified themselves as Estonians. As Estonia is promoted as one of the top countries in cybersecurity in Europe and globally (Rikk et al., 2022), Estonians may be more aware of the importance of cybersecurity.

There were two questions to evaluate general cybersecurity knowledge among TES employees and whether they had previous experiences with the 2FA system. The majority (84%) answered that they had previous experience with the 2FA, and they also thought that using the 2FA system was a good, wise idea and would like to use the 2FA system in their job. 93% of respondents agreed or strongly agreed that cybersecurity is important to them. The main questions used to assess attitudes and motivation were divided into four sections, each consisting of several questions: Performance Expectancy, Effort Expectancy, Social Influence, and Facilitating conditions.

Performance Expectancy

The results of performance expectancy among TES employees were primarily favorable. People agreed that the 2FA system is helpful for organizations, and from their point of view, on how useful a system is to them, most responses were also positive (Figure 1).

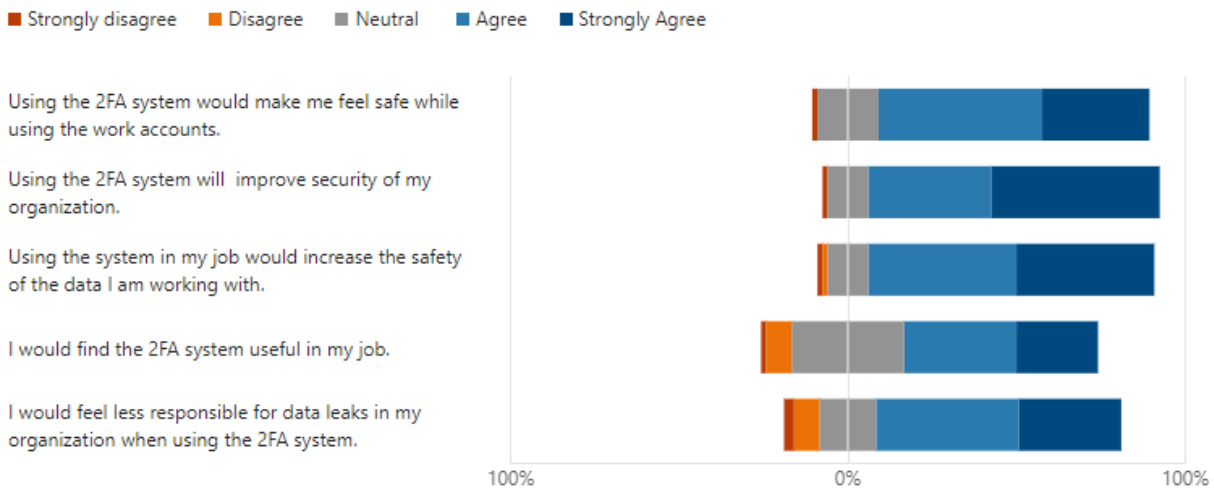


Figure 1. Performance Expectancy
Source: Microsoft Forms, calculations/on the basis of data shown in appendix 1. compiled by the author

80 % of respondents strongly agreed or agreed with the statement, "Using the 2FA system would make me feel safe while using the work accounts." 86 % of respondents agreed or strongly agreed that using the 2FA system would improve their organization's security. 85 % agreed or strongly agreed that the 2FA system would increase the safety of the data they are working with. 58 % of respondents agreed or strongly agreed with finding the 2FA useful system in their job. 73 % agreed or strongly agreed that they would feel less responsible for data leaks in their organization when using the 2FA system. Less than 2% of the respondents strongly disagreed that the 2FA system would make them feel safe while working with school accounts. The most disagreements occurred in the last two questions of Performance Expectancy, although the general percentage of disagreement is still low.

In general, the results are positive in the Performance Expectancy section. Participants' answers to question 4 were the most diverse. This might be influenced by the system's Effort expectancy and Ease of use, which will be discussed in the next section, where effort expectancy is analyzed more closely. The respondents who agreed with the statements were also primarily optimistic about the other statements related to the Attitude questions at the end of the questionnaire. Noticable is that one 40-44-year-old male respondent strongly disagreed with all Performance Expectancy statements. Although he has previous experiences and thinks cybersecurity is extremely important, he finds it useless in his work. He thinks the system is unreliable because it belongs to someone other than TES.

Effort expectancy

The results for the Effort expectancy section were also mostly positive (Figure 2). Most respondents (76%) agreed or strongly agreed that they would learn the system easily. 80,5% of the participants believe the 2FA system would be clear and understandable. 77,5 % of TES employees agreed or strongly agreed with the statement," It would be easy for me to become skillful at using the 2FA system". The same percentage of people found the 2F system easy to use. None of the TES employees strongly disagreed with any of the statements in the effort expectancy section. Of all respondents, 9.5% disagreed with "I would find the system easy to use," and more than half of these participants did not have previous experience with the 2FA system, so therefore the respondents may feel that the 2FA system is difficult to use. Most respondents who did not find the system easy to use still think the 2FA system is a good and wise idea. Although all of them answered that it would be unpleasant to use it, they also agreed that the 2FA system would improve the security of TES.

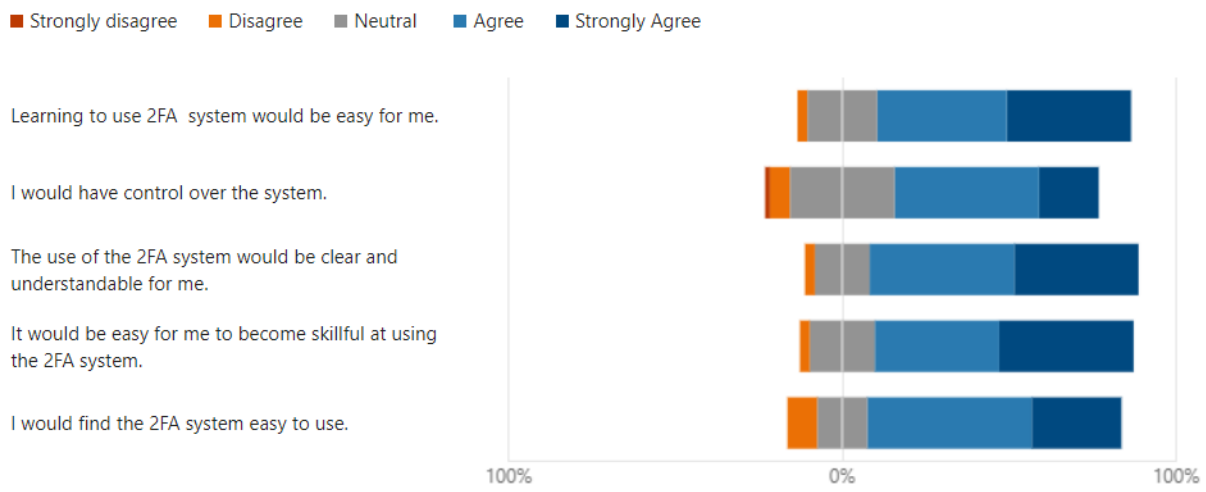


Figure 2. Effort Expectancy
Source: Calculations/based on data shown in appendix 2. compiled by the author

Six respondents disagreed or strongly disagreed with "I would find the 2FA system useful in my job." In addition, half of them did not find the 2FA system easy to use, while the other half agreed that the system would be easy to use. Most of them disliked the idea of using 2FA in their organization, and all thought that using the 2FA system would be unpleasant. According to the theory, Ease of use could influence Usefulness, Attitude, and Motivation toward new technological

updates. In this case, even if some employees could easily use the system, some of them would still not like implementing it. Overall, more than 75% of each statement in the section on Effort expectancy was answered positively, and TES employees found the 2FA system easy to learn and use.

Social influence

In the Social influence section, the answers varied the most (Figure3). 63 % of the TES employees agreed or strongly agreed that if people who are important to them think they should use the system, they will. 10,5 % of the respondents disagreed or strongly disagreed with the statement. The other question was whether people who are important to the person think that they should not use the system will not. More than half (54 %) disagreed or strongly disagreed with the statement and only 18 % agreed. Most TES employees would like to try the system even if close people do not recommend it, and when a trustworthy person suggests trying, they are most likely to do it.

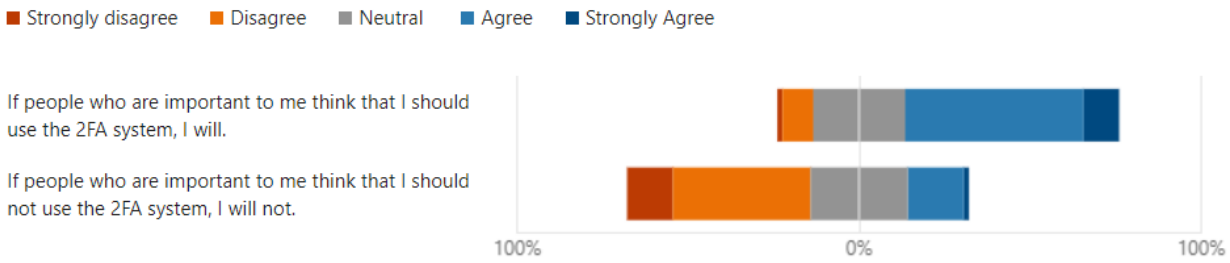


Figure 3. Social Influence
Source: Calculations/on the basis of data shown in appendix 3. compiled by the author

Facilitating conditions

70,2% of people said that they had the necessary devices to use the 2FA system (Figure 4). This study focused on a 2FA system related to phones as personal devices. The comments added by the respondents indicated that people were most concerned about device issues. 33% of respondents who added the comments at the end of the questionnaire mentioned "*phone"* in their comments. TES employees are worried about what happens if the phone is left at home or runs out of battery, for instance, or if the phone is old (not a smartphone). One respondent disliked the idea of the school accounts being linked to his personal phone. Another question the respondents asked was, if a person has a non-Estonian phone number, is it still possible to use the system? One more technical problem was noticed based on previous experience. A person had trouble receiving the required codes for the 2FA system on his phone. However, the same person would still like the idea of using the 2FA system.

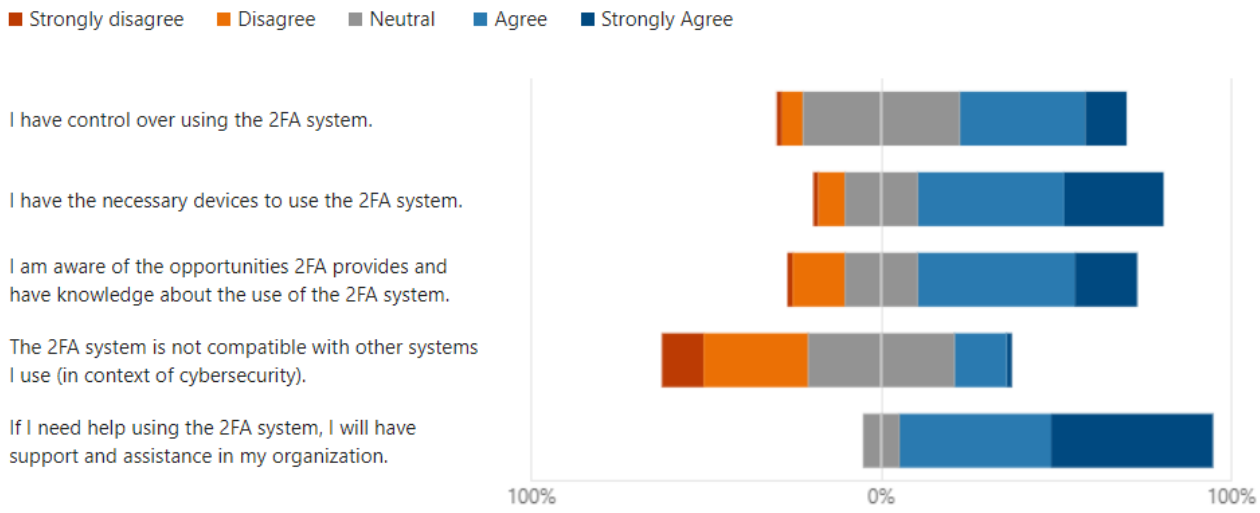


Figure 4. Facilitating Conditions
Source: Calculations/on the basis of data shown in appendix 4. compiled by the author

Although most respondents answered that they had the necessary device, the interpretation of the question might differ. Some respondents understood it as a physical device that they had, and some considered the Estonian phone number and running of the battery or old device as an issue. 16, 5% of people disagreed that they were aware of the opportunities 2FA provided and knew about using the 2FA system. However, 7 out of 11 respondents had previous experience using the 2FA system. 63 % of the TES employees agreed or strongly agreed with this statement.

42 % of respondents find the 2FA system compatible somehow with the other system they use at work, and 16,5% agreed that "The 2FA system is incompatible with other systems I use ".When TES employees were asked if they would need help using the 2FA system and if they felt they had support and assistance in their organization, the answer was clear. Almost 90% of the participants agreed or strongly agreed, and none disagreed. Overall, the section on facilitating conditions was positively answered. Employees have the required devices, knowledge, significant support, and assistance in TES for using the new digital update.

Total percentage of all responses by thematical groups

The level of agreement with the statements of Effort expectancy, Performance expectancy, and Facilitating conditions ranged from 79% to 94%. 94% of the respondents either agreed or strongly agreed with all the performance expectancy statements, and 6,4% disagreed or strongly disagreed with the same statements. The response "neutral" was left out because it does not give good value in general agreement and disagreement discussion. 94 % of the TES employees agreed or strongly agreed with all effort expectancy statements, and 6 % disagreed.

79 % of the respondents neither agreed nor strongly agreed with all the facilitating conditions questions, and 21 % disagreed. The percentage in facilitating conditions is lower due to the one question, "The 2FA system is not compatible with other systems I use". The question was posed in a negative form; 41% of respondents disagreed or strongly disagreed with the statement, so they thought the 2FA system was compatible with other systems they used. Looking at all the responses, we can claim that TES employees positively evaluate these three areas. They see the system's usefulness and are willing to try and learn the system.

The Social influence results differ from the previous blocks. The level of total agreement was 79, 3%, and 20,5% disagreed or strongly disagreed. Although people mostly agreed that if important people suggest using the system, they will, they disagreed (53,7%) with the second statement, "If people who are important to me think that I should not use the 2FA system, I will not." TES employees are willing to try the system even if others do not recommend it.

Percentage of the male and female responses by thematical groups

The percentage of female and male responses to all the questions in each thematical group were analyzed. The "neutral" was also not considered, and only "strongly agreed, agreed, disagreed, strongly disagreed" were analyzed. The agreement with performance expectancy was 95% among female TES employees. 92,4% of female respondents agreed with the effort statements as well. None of the female respondents did mark "strongly disagree" on any of the statements in these two blocks of questions. TES female employees find the 2FA system useful and are willing to try it at their workplace.

72,98% of male respondents agreed or strongly agreed with performance expectancy statements. The results are lower than among women. The total percentage of agreement among men in the effort expectancy block was 79,5%. To compare the results, men in TES are less favorable toward the 2FA system than women, although the agreement level is still high. In facilitating conditions, around 77% of men and women agreed with the statements, so most think they have the needed devices, knowledge, and support to use the 2FA system.

57% of female employees agreed or strongly agreed with the social expectancy statement, and 42,8% disagreed or strongly disagreed with the statements (Appendix 3). In the social influence section, it is more valuable to analyze the questions separately because similar statements were asked in a way that the total percentage gives little information. The first statement was, " If people who are important to me think I should use the 2FA system, I will, " 71% of female respondents agreed or strongly agreed, and 14% disagreed (0 strongly disagreed). With the second statement, "If people who are important to me think that I should not use the 2FA system, I will not," 72 % of female employees disagreed or strongly disagreed, and 29% agreed (0 strongly agreed).

The Social Influence among TES men employees was analyzed the same way as it was done with the female above (two statements separately). 70% of men agreed or strongly agreed with the first statement and will try the system if others recommend it, 30% disagreed, and 70% of TES male employees disagreed with the second statement. The only difference between men and women in the social influence section was that TES men employees had 30% of disagreement on the first question, which is higher than among female employees (14%). Social influence among TES men and women is visible . If close and important people recommend using the system, they will try it. Nevertheless, in the second question, the social influence is weaker among both men and women

than in the first statement because TES employees want to try the 2FA system even without other people's disapproval.

Percentage of the responses based on nationality by thematical groups

To analyze the differences between nationalities in how they answered the questions, the respondents were divided into Estonians (33 respondents) and others (34) because the number of Estonian respondents was primarily much more significant than the other nationalities individually. The responses were also calculated in the total percentage to determine the percentage of agreement and disagreement among all respondents. Option "neutral" was not included in the calculations.

In the Performance expectancy section, 97 % of Estonian respondents and 81,5% of others agreed or strongly agreed with all the statements. The percentage of agreement is high, but the difference occurs in disagreements. 18,5 % of TES employees with different nationalities disagreed and strongly disagreed, and only 2 % of Estonians disagreed with performance expectancy statements. That shows that almost all Estonian employees in TES think using the 2FA system is useful. Next is effort expectancy, where the percentage of all Estonian employees who agreed or strongly agreed was 89 %, and 84 % was for the others. The results are pretty even here as well. 79 % of TES Estonian employees agreed or strongly agreed with the facilitating conditions statements, and 74,7% of multiple nationalities among TES employees also found an agreement with those questions.

In the Social Influence category, the percentage in agreement statements was similar among TES Estonian employees and employees with multiple other nationalities. 58% of Estonians agreed or strongly agreed with both social influence statements. The percentage of disagreement was 41%. The other nationalities responded with 55% of agreement and 45% disagreement. The questions were analyzed separately because each statement gives a more specific overview of the results in this category. In the first statement on Social Influence, 88% of Estonian employees agreed that they would try the new system if important people recommended it (0% strongly disagreed). Almost the same percentage, 85% among others, agreed or strongly agreed with the same statement, and disagreement was also similar (12% of Estonians and 14% of other nationalities). The second statement was almost equal between nationalities. 73% of Estonians and 72% of others disagreed or strongly disagreed with the statement, "If people who are important to me think that

I should not use the system, I will not." Also, the agreement percentage range was almost the same on the same statement (26-28%) among Estonians and others. Therefore no significant differences in Social Influence between the two different nationality groups did not occur. Both Estonian and other multiple nationalities are willing to try the new update with or without the recommendations of other important people.

General Attitude questions

The general questions were asked to evaluate motivation and attitude toward the 2FA system. 94% of the respondents answered that using the 2FA system is a good and wise idea. 85% of TES employees like the idea of using the 2FA system. 4 % (six people) think that using the system is a bad idea, and three out of those four people dislike the idea of using the 2FA system in their work. They also find that using the 2FA system will be unpleasant, and in general, the idea is foolish. Even when people think that using the 2FA system in TES is a good idea, only 48% find that using the 2FA system will be pleasant, and all of them like the idea of using 2FA in their workplace. In the statement, “Using the system will be unpleasant,” 40 % of respondents agreed. Although 15 % (10 respondents) disliked the idea of using a 2FA system, the majority of them, think that cybersecurity is extremely important to them.

Summary

The overall results are very positive, and there are no significant conflicts or reasons for not implementing the 2FA system. Most TES employees believe that cybersecurity is an extremely important topic. Therefore they believe in the need for the new system. They are willing to try even if they do not have previous experience with the system. Although social influence is an essential factor in technology acceptance, this study shows that TES employees are influenced by important and close people when they are encouraged to try the system. However, when people recommended not to do that, respondents disagreed and still wanted to try it.

In the added comments, people's biggest concern was related to their personal devices. They were worried about what happens when they forget their phone at home and must sign in to the work account and if the phone number is non-Estonian. One person pointed out, *"We cannot rely on a system that uses technology that does not belong to TES, and that is known for being a target of big data companies. Beware!"* The same person strongly disagreed on all performance and effort expectancy questions and responded that it is easy for him to learn the 2FA system. However, he is against using it at TES- this was only negative feedback from the comments. Other employees pointed out that they understand the system's benefits. Although it could be annoying, time-consuming, and requires extra clicks during the day, the advantages of using the 2FA system outweigh the disadvantages. Most TES employees find the system useful and believe that they will become skillful in using it. Even if they have issues with using the new 2FA system, they feel they have full support and needed help from the organization.

CONCLUSION

Several factors make TES employees accept or reject the new technological change. The study shows that attitudes and motivations, previous experience, social influence, and knowledge are the main determinants creating the behavior toward the new system among TES employees. The factors that make TES employees reject or accept technological updates/changes were evaluated through an example of two-factor authentication.

Throughout the study, *Perceived Usefulness* and *Perceived Ease of Use* are the most important factors influencing people's opinions and behaviors. The main part of the questionnaire was divided into four groups of statements: *Performance Expectancy, Effort Expectancy, Facilitating Conditions,* and *Social Influence.* The Performance expectancy in the case of this study is described from the Usefulness point of view, and Effort expectancy is considered as Ease of use were also main determinants in technology acceptance in TES. Most TES employees acknowledged the system's benefits, even if they had not had previous experiences with it. They responded that they would feel more secure in their organization and are willing to test the new system even if others do not recommend it. They also believe they have all the needed support in using the system, even if they believe it is unpleasant. The Usefulness is more important than Ease of use in the case of the given study and the importance of cybersecurity was considered above comfort.

Most of the TES employees found the 2FA a valuable system for their organization. As most of the respondents were in the age group 30-39 years old, the other age groups could not be compared because the number of respondents was too small in other groups to generalize and make conclusions. Nationalities were analyzed separately in two groups - Estonian and Others (multiple nationalities) and those two nationality groups found no significant differences in attitudes and motivations toward the new technological update.

The importance of cybersecurity, which creates the attitude and motivation, are the factors that make TES employees accept or reject new technological change. Attitude, gender, and age were

not the main determinants of attitude in the case of this study, but were necessary to observe. The results show that TES teachers and staff members are generally ready for technological change and would like to implement it in their work. As the research results were positive, the research results and the support of employees will encourage the TES administration to implement the change shortly. Also, needed policies should be added to the regulations of TES. It is possible to share the results of this research with other schools since TES is the first school to implement two-factor authentication and evaluate employee attitudes toward implementing this technology. It gives value to implementing technology in an organization because the study results are positive, and employees consider the technology essential to adopt. No crucial objections were discovered regarding why not to implement the 2FA system. The only noticeable remark is that the response rate is lower than expected, and it could also show people's interest in the topic. Others who did not respond to the questionnaire may not have considered the topic important.

The research did not include other European schools because they operate in different countries with different levels of digital competence and local countries' legislation. First, it was important to test employees of the same school with the same knowledge of the organization's IT rules set up by the school's IT- Policy, and if the results were successful, spread them to other European Schools. The research results will inform other European schools about employees' attitudes and motivations toward new technology or system updates in TES. The research benefits other ES schools willing to implement the 2FA authentication or implement changes in the cybersecurity field in general. As the main focus is to study people's attitudes and motivations when adopting new technologies, the future of this work can be a more extensive study in the European school system (other ES schools) to determine general attitudes regarding cybersecurity and digital competencies.

LIST OF REFERENCES

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. *Action Control. SSSP Springer Series in Social Psychology*, 11–39. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-t

Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Prentice Hall.

Ajzen, I., & Fishbein, M. (2000). Attitudes and the Attitude-Behavior Relation: Reasoned and Automatic Processes. *European Review of Social Psychology*, *11*(1), 1–33. https://doi.org/10.1080/14792779943000116

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

Chuttur, M. (2009). Overview of the Technology Acceptance Model: Origins, Developments and Future Directions. *All Sprouts Content*, *9*(37). https://aisel.aisnet.org/sprouts_all/290/?utm_source=aisel.aisnet.org%2Fsprouts_all%2F290&utm_medium=PDF&utm_campaign=PDFCoverPages

Davis, F. D. (1985). *A Technology Acceptance Model For Empirically Testing Ned End- User Information Systems: Theory And Results* [PhD in Management]. Massachusetts Institute of Technology.
Retrieved from: https://www.researchgate.net/publication/35465050

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *Management Information Systems Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982–1003. https://www.jstor.org/stable/2632151

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behaviour*, *61*, 656–666. https://doi.org/10.1016/j.chb.2016.03.068

Ellerbeck, S. (2023, July 26). *Nearly half of organizations are being hit by economic crime, with cybercrime the gravest threat. What can they do about it?* World Economic Forum. Retrieved March 23, 2023, from https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Addison-Wesley. https://people.umass.edu/aizen/f&a1975.html

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital Identity Guidelines. *National Institute of Standards and Technology, U.S Department of Commerce*, *800*(63–3). https://doi.org/10.6028/NIST.SP.800-63-3

Hicock, R. (2018, October 17). *Password Guidance - Microsoft Research*. Microsoft Research. Retrieved April 10, 2023, from https://www.microsoft.com/enus/research/publication/password-guidance/

Hirschheim, R. (2007). Introduction to the Special Issue on "Quo Vadis TAM – Issues and Reflections on Technology Acceptance Research." *Journal of the Association for Information Systems*, *8*(4). https://doi.org/10.17705/1jais.00128

Horowitz, M. (2022). Cyber Attack Trends: Check Point´s 2022 Mid-Year Report. In *Checkpoint*. Checkpoint. Retrieved March 23, 2023, from https://www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2022.pdf

Jeong, J., Christina Oliver, G., Mihelcic, J., & Rudolph, C. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. *Conference Paper*, 2-8. https://doi.org/10.1109/CIC48465.2019.00047

Jones, C. J. (2023, March 28). *50 Identity And Access Security Stats You Should Know In 2023*. Expert Insights. Retrieved April 10, 2023, from https://expertinsights.com/insights/50-identity-and-access-security-stats-you-should-know/

Kim, I., Kim, Y., & Han, H. (2008). The effects of perceived risk and technology type on users' acceptance of technologies. *Information and Management*, *45*(1), 1–9. https://doi.org/10.1016/j.im.2007.03.005

King, W. P., & He, J. (2006). A meta-analysis of the technology acceptance model. *Information & Management*, *43*(6), 740–755. https://doi.org/10.1016/j.im.2006.05.003

Kwekuako. (2023, March 16). *Password policy recommendations - Microsoft 365 admin*. Microsoft Learn. https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

Lai, P. C. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management*, *14*(1), 21- 38. https://doi.org/10.4301/s1807-17752017000100002

Magalhaes, M. M. (2018, December 20). *Security Vs. Usability: Does There Have To Be A Compromise?* Techenix. Retrieved April 9, 2023, from https://techgenix.com/security-vs-usability/

Marangunić, N., & Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal Access in the Information Society*, *14*(1), 81–95. https://doi.org/10.1007/s10209-014-0348-1

Microsoft. (2023). *What is two-factor authentication (2FA)? | Microsoft Security*. Microsoft. Retrieved April 8, 2023, from https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa

Ministry of Education and Research. (2021). Education Strategy 2021-2035. In *Ministry of Education and Research, Republic of Estonia*. Retrieved April 6, 2023, from https://www.hm.ee/ministeerium-uudised-ja-kontakt/ministeerium/strateegilised-alusdokumendid-ja-programmid?view_instance=0¤t_page=1#haridusvaldkonna-are

Morris, M. A., & Venkatesh, V. (2000). Age differances in technology adoption decisions: Implications for a changing work force. *Personnel Psychology*, *53*(2), 375–403. https://doi.org/10.1111/j.1744-6570.2000.tb00206.x

Morris, M. G., Venkatesh, V., & Ackerman, P. L. (2005). Gender and Age Differences in Employee Decisions About New Technology: An Extension to the Theory of Planned Behavior. *IEEE Transactions on Engineering Management*, *52*(1), 69–84. https://doi.org/10.1109/tem.2004.839967

Mustafa, A. S., & Garcia, M. (2021). Theories Integrated With Technology Acceptance Model (TAM) in Online Learning Acceptance and Continuance Intention: A Systematic Review. *2021 1st Conference on Online Teaching for Mobile Education (OT4ME)*. https://doi.org/10.1109/ot4me53559.2021.9638934

Office of the Secretary-General of the European Schools. (n.d.). Office of the Secretary- General of the European Schools. Retrieved March 9, 2023, from https://www.eursc.eu/en

Office of the Secretary-General [Pedagogical Development Unit]. (2018). Key Competences for Lifelong Learning in the European Schools. In *https://www.eursc.eu/BasicTexts/2018-09-D-69-en-2.pdf* (No. 2018-09-D-69-en-2). Office of the Secretary-General. Retrieved March 22, 2023, from https://www.eursc.eu/BasicTexts/2018-09-D-69-en-2.pdf

Pavlou, P. A., & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *Management Information Systems Quarterly*, *30*(1), 115. https://doi.org/10.2307/25148720

PricewaterhouseCoopers. (2022). *PwC's Global Economic Crime and Fraud Survey 2022*. PwC. Retrieved March 23, 2023, from https://www.pwc.com/fraudsurvey

RIA. (2022). *The RIA yearbook: 2021 was a year of security vulnerabilities | RIA*. Information System Authority. https://ria.ee/en/news/ria-yearbook-2021-was-year-security-vulnerabilities

RIA. (2023). *Cyber Security in Estonia 2023*. Information System Aurhority. https://www.ria.ee/media/2653/download

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Plannning*, *27*(2), 23–39. http://isep.info/educational-planning-journal

Rikk, R., Sepp, T., & Ainge, K. (2022, July). *Estonia*. National Cybersecurity Index. Retrieved April 28, 2023, from https://www.ncsi.ega.ee/country/ee/

Shachak, A. S., Kuziemsky, C. E., & Petersen, C. (2019). Beyond TAM and UTAUT: Future directions for HIT implementation research. *Journal of Biomedical Informatics*, *100*. https://doi.org/10.1016/j.jbi.2019.103315

Straub, E. T. (2009). Understanding Technology Adoption: Theory and Future Directions for Informal Learning. *Review of Educational Research*, *79*(2), 625–649. https://www.jstor.org/stable/40469051

Taherdoost, H. (2019). Importance of Technology Acceptance Assessment for Successful Implementation and Development of New Technologies. *Global Journal of Engineering Sciences*, *1*(3). https://doi.org/10.33552/gjes.2019.01.000511

Tallinn European School. (2022, January 31). *Information Technology (IT)- Policy*. Retrieved March 23, 2023, from https://tes.edu.ee/discovertes/school-documents/

Tallinn European School. (2023, January 11). *Tallinn European School*. Retrieved March 4, 2023, from https://tes.edu.ee/

Taylor, S., & Todd, P. (1995). Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research*, *6*(2), 144–176. https://www.jstor.org/stable/23011007

The Organisation for Economic Co-operation and Development [OECD]. (2022). PISA for Schools How The European Schools Compare Internationally 2022. In *https://www.eursc.eu/en/Office/reports-statistics*. OECD.

Use stronger security than passwords alone: Your Password Doesn´t Matter (By A. W. Weinert). (n.d.). [Video]. Microsoft. Retrieved April 10, 2023, from https://www.microsoft.com/en-us/videoplayer/embed/RE4xtwr?culture=en-us&country=us

Venkatesh, M., Morris, M., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 428–478.

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Weinert, A. W. (2023, January). 2023 identity security trends and solutions from Microsoft. *Microsoft*. Retrieved April 9, 2023, from https://www.microsoft.com/en-us/security/blog/2023/01/26/2023-identity-security-trends-and-solutions-from-microsoft/

Why Human Error is #1 Cyber Security Threat to Businesses in 2021. (2021, February 4). *The Hackers News*. Retrieved April 10, 2023, from https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html#:~:text

World Economic Forum. (2022). The Global Risks Report 2022, 17th Edition. In *World Economic Forum* (ISBN: 978-2-940631-09-4). World Economic Forum. Retrieved March 16, 2023, from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

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

APPENDICES

Appendix 1. Performance expectancy

Responses to all Performance Expectancy statements

Using the 2FA system would make me feel safe while using the work accounts.	Count of Responses	Percentage of each question
Agree	33	49.25%
Neutral	12	17.91%
Strongly Agree	21	31.34%
Strongly disagree	1	1.49%
Grand Total	67	100%
Using the 2FA system will improve security of my organization.		
Agree	24	35.82%
Neutral	8	11.94%
Strongly Agree	34	50.75%
Strongly disagree	1	1.49%
Grand Total	67	
Using the system in my job would increase the safety of the data I am working with.		
Agree	30	44.78%
Disagree	1	1.49%
Neutral	8	11.94%
Strongly Agree	27	40.30%
Strongly disagree	1	1.49%
Grand Total	67	
I would find the 2FA system useful in my job.		
Agree	23	34.33%
Disagree	5	7.46%
Neutral	22	32.84%
Strongly Agree	16	23.88%
Strongly disagree	1	1.49%
Grand Total	67	

I would feel less responsible for data leaks in my organization when using the 2FA system.		
Agree	29	43.28%
Disagree	5	7.46%
Neutral	11	16.42%
Strongly Agree	20	29.85%
Strongly disagree	2	2.99%
Grand Total	67	

Source: Author's calculations, based on survey results

Percentage of total responses of Performance Expectancy statements

Strongly Agree	118	43.07%
Strongly disagree	6	2.19%
Agree	139	50.73%
Disagree	11	4.01%
Total responses	274	

Source: Author's calculations, based on survey results

Percentage of Male and Female responses (Performance expectancy)

Female	Respondents	Percentage		Male	Respondents	Percentage
Strongly Agree	50	41.67%		Strongly Agree	14	37.84%
Strongly disagree	1	0.83%		Strongly disagree	5	13.51%
Agree	64	53.33%		Agree	13	35.14%
Disagree	5	4.17%		Disagree	5	13.51%
Total	120				37	

Source: Author's calculations, based on survey results

Respondents based on nationality (Estonians, Other)

	Estonians	Other	EST(percentage)	OTHER(Percentage)
Strongly Agree	35	32	41.67%	39.51%
Strongly disagree	0	6	0.00%	7.41%
Agree	47	34	55.95%	41.98%
Disagree	2	9	2.38%	11.11%
Total responses	84	81	100%	100%

Source: Author's calculations, based on survey results

Appendix 2. Effort Expectancy

Responses to all Effort Expectancy statements

Learning to use 2FA system would be easy for me.	Count of Responses	Percentage
Agree	26	39%
Disagree	2	3%
Neutral	14	20,9%
Strongly Agree	25	37,3%
Grand Total	67	
I would have control over the system.		
Agree	29	43%
Disagree	4	6%
Neutral	21	31,3%
Strongly Agree	12	17,9%
Strongly disagree	1	1,5%
Grand Total	67	
The use of the 2FA system would be clear and understandable for me.		
Agree	29	43,3%
Disagree	2	3%
Neutral	11	16,4%
Strongly Agree	25	37,3%
Grand Total	67	
It would be easy for me to become skillful at using the 2FA system.		
Agree	25	37,3%
Disagree	2	3%
Neutral	13	19,4%
Strongly Agree	27	40,3%
Grand Total	67	
I would find the 2FA system easy to use.		
Agree	33	49,2%

Disagree	6	9%
Neutral	10	14,9%
Strongly Agree	18	26,9%
Grand Total	67	

Source: Author's calculations, based on survey results

Percentage of total responses of all Effort Expectancy statements

Strongly Agree	107	40.23%
Strongly disagree	1	0.38%
Agree	142	53.38%
Disagree	16	6.02%
	266	100.00%

Source: Author's calculations, based on survey results

Percentage of Male and Female responses (Effort expectancy)

Female	Respondents	Percentage		Male	Respondents	Percentage
Strongly Agree	32	34.78%		Strongly Agree	22	50.00%
Strongly disagree	0	0.00%		Strongly disagree	1	2.27%
Agree	53	57.61%		Agree	13	29.55%
Disagree	7	7.61%		Disagree	8	18.18%
Total	92	100%		Total	44	100%

Source: Author's calculations, based on survey results

Respondents based on nationality (Estonians, Other)

	Estonians	Other	EST(Percentage)	OTHER (Percentage)
Strongly Agree	27	6	42.19%	12.24%
Strongly disagree	0	0	0.00%	0.00%
Agree	30	35	46.88%	71.43%
Disagree	7	8	10.94%	16.33%
Total responses	64	49	100%	100%

Source: Author's calculations, based on survey results

Appendix 3. Social Influence

Responses to all Social Influence Statements

If people who are important to me think that I should use the 2FA system, I will.	Count of Responses
Agree	35
Disagree	6
Neutral	18
Strongly Agree	7
Strongly disagree	1
Grand Total	67
If people who are important to me think that I should not use the 2FA system, I will not.	
Agree	11
Disagree	27
Neutral	19
Strongly Agree	1
Strongly disagree	9
Grand Total	67

Source: Author's calculations, based on survey results

Percentage of total responses of all Social Influence statements

Strongly Agree	8	8.25%
Strongly disagree	10	10.31%
Agree	46	47.42%
Disagree	33	34.02%
Total	97	100.00%

Source: Author's calculations, based on survey results

TES female responses in Social Influence statements

1.If people who are important to me think that I should use the 2FA system, I will	Female Respondents	Percentage
Strongly Agree	4	57%
Strongly disagree	0	0%
Agree	2	29%
Disagree	1	14%
Total	**7**	100%
2. If people who are important to me think that I should not use the 2FA system, I will not		
Strongly Agree	0	0%
Strongly disagree	2	29%
Agree	2	29%
Disagree	3	43%

Total	**7**	100%

Source: Author's calculations, based on survey results

TES male responses in Social Influence statements

1.If people who are important to me think that I should use the 2FA system, I will	Male Respondents	Percentage
Strongly Agree	1	10%
Strongly disagree	1	10%
Agree	6	60%
Disagree	2	20%
Total	10	100%
If people who are important to me think that I should not use the 2FA system, I will not		
Strongly Agree	1	10%
Strongly disagree	1	10%
Agree	2	20%
Disagree	6	60%
Total	10	100%

Source: Author's calculations, based on survey results

The responses of two nationality groups- Estonians and others

Social Influence in Total	EST	Percentage	Other	Percentage
Strongly Agree	5	10%	3	7.14%
Strongly disagree	5	10%	4	9.52%
Agree	23	48%	20	47.62%
Disagree	15	31%	15	35.71%
1.If people who are important to me think that I should use the 2FA system, I will.	EST	Percentage	Other	Percentage
Strongly Agree	5	20.00%	2	10.00%
Strongly disagree	0	0.00%	1	5.00%
Agree	17	68.00%	15	75.00%
Disagree	3	12.00%	2	10.00%
Total responses	25	100.00%	20	100.00%
2. If people who are important to me think that I should not use the 2FA system, I will not.	EST	Percentage	Other	Percentage
Strongly Agree	0	0.00%	1	4.55%
Strongly disagree	5	21.74%	3	13.64%
Agree	6	26.09%	5	22.73%
Disagree	12	52.17%	13	59.09%
Total responses	23	100.00%	22	100.00%

Source: Author’s calculations, based on survey results

Appendix 4. Facilitating Conditions

Responses to all Performance Expectancy statements

I have control over using the 2FA system.	Count of Responses	Percentage
Agree	24	35,6%
Disagree	4	6%
Neutral	30	44,8%
Strongly Agree	8	12%
Strongly disagree	1	1,6%
Grand Total	67	
I have the necessary devices to use the 2FA system.		
Agree	28	41,8%
Disagree	5	7.50%
Neutral	14	20,9%
Strongly Agree	19	28,4%
Strongly disagree	1	1.50%
Grand Total	67	
I am aware of the opportunities 2FA provides and have knowledge about the use of the 2FA system.		
Agree	30	44,8%
Disagree	10	14,9%
Neutral	14	20,9%
Strongly Agree	12	17,8%
Strongly disagree	1	1,6%
Grand Total	67	
The 2FA system is not compatible with other systems I use (in context of cybersecurity).		
Agree	10	14,9%
Disagree	20	29,9%
Neutral	28	41,8%
Strongly Agree	1	1.50%
Strongly disagree	8	26,9%
Grand Total	67	

If I need help using the 2FA system, I will have support and assistance in my organization.		
Agree	29	43,3%
Neutral	7	10,5%
Strongly Agree	31	46,2%
Grand Total	67	

Source: Author's calculations, based on survey results

Percentage of total responses of all Facilitating Conditions statements

Strongly Agree	71	29.34%
Strongly disagree	11	4.55%
Agree	121	50.00%
Disagree	39	16.12%
Total	242	100.00%

Source: Author's calculations, based on survey results

Percentage of Male and Female responses (Facilitating Conditions)

Female	Respondents	Percentage		Male	Respondents	Percentage
Strongly Agree	20	19.80%		Strongly Agree	22	42.31%
Strongly disagree	3	2.97%		Strongly disagree	5	9.62%
Agree	58	57.43%		Agree	18	34.62%
Disagree	20	19.80%		Disagree	7	13.46%
Total	101			Total	52	

Source: Author's calculations, based on survey results

Respondents based on nationality (Estonians, Other)

	Estonians	Other	EST(Percentage)	OTHER(Percentage)
Strongly Agree	34	32	34.69%	32.32%
Strongly disagree	6	5	6.12%	5.05%
Agree	44	42	44.90%	42.42%
Disagree	14	20	14.29%	20.20%
Total responses	98	99	100%	100%

Source: Author's calculations, based on survey results

Appendix 5. Comments and relevant graphics

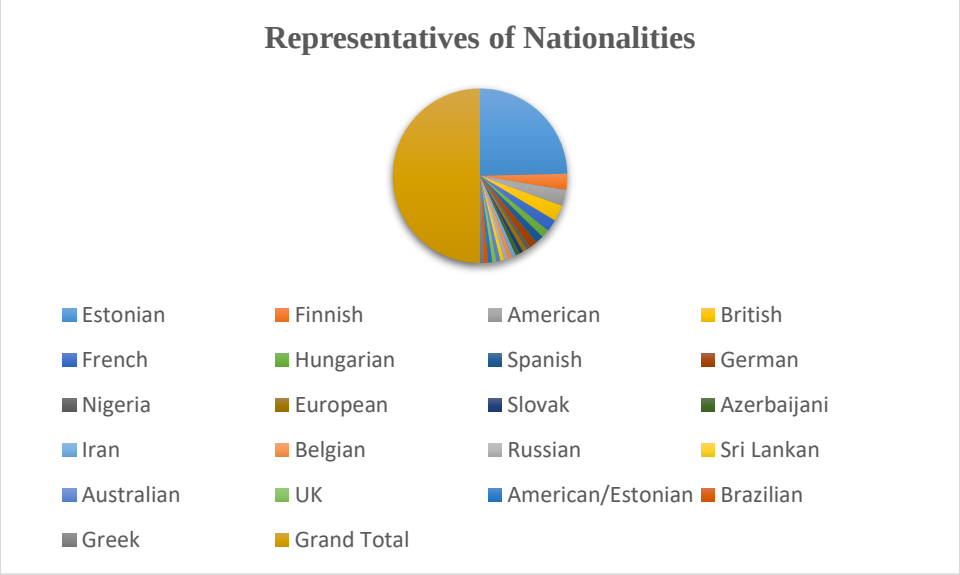
TES employees' comments (optional for respondents)

Number	Comments
1	Is there some kind of back up where if your phone wasn't with you one time at school you could still use MySchool?
2	I am very happy to use 2FA, BUT!!! my current mobile phone is getting old and it doesnt work with some apps any more. Therefore, I feat that I will have to buy a new phone just for the 2PA (otherwise I am still happy with my current phone). So, if it is granted, that I dont need to have the newest phone, I think 2FA is a very good solution.
3	Great idea - I am not a fan of having school systems linked to my phone is all.
4	The only concern I have is, what happens if I forget my phone at home and need to sign in to my work environment?
5	Considering the number of people and their different background, the initial implementation of 2FA would be a challenge and would require extra support from the IT team but as the pros of using 2FA overweigh the cons, it is absolutely doable with the support of the management and with time it should become second nature to users.
6	We cannot relay on a system that uses technology that does not belong to TES and that it is known for being target of big data companies. Beware!
7	I don't like anything which takes more time. Daily use in 2FA system would be time demanding for me because it requires many extra clicks during the day.
8	I am more than willing to use the 2FA system, but I am not sure if it works with a non-Estonian phone number (as I am teaching remotely from Greece and only have a Greek SIM card). If so, then all good!
9	I think that the idea in general it is good to secure the system, although it is annoying in use.

10	It can be too time consuming to use every time when open the computer.
11	I feel neutral in regard of the 2FA system being pleasant or unpleasant. I think it is important to implement it, as it contributes to the cybersecurity of our school. So, I understand the benefits and do not care if it makes it more difficult (or unpleasant) to log in.
13	I don't have to like using the 2FA system, but if it contributes to security, of course I have to use it
14	I don't mind this either way, but I have had trouble received codes with this system before. It could also be problematic if someone forget their phone at work or runs out of battery.
15	I understand that it makes my data more secure, but the extra steps in logging in is time consuming and will annoy me.
16	I have to try it first, then I can evalaute how easy it is for me.
17	Thank you for the survey. This is a vital topic. Good luck for the research. :)

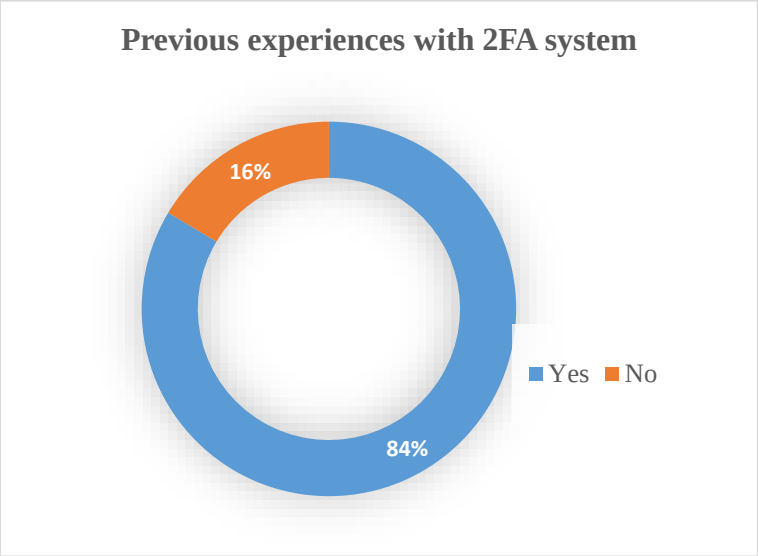
Source: Microsoft Forms (2023), TES employee's comments, data gathered by author

Representatives of nationalities



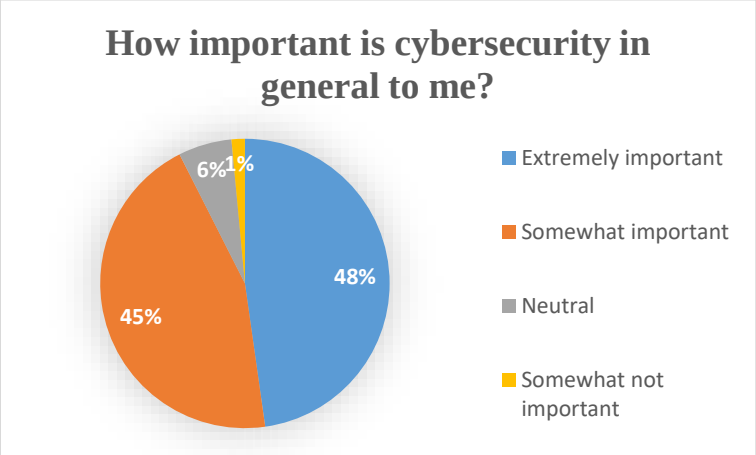
Source: Author's calculations, based on survey results

Previous experiences with the 2FA system among TES employees



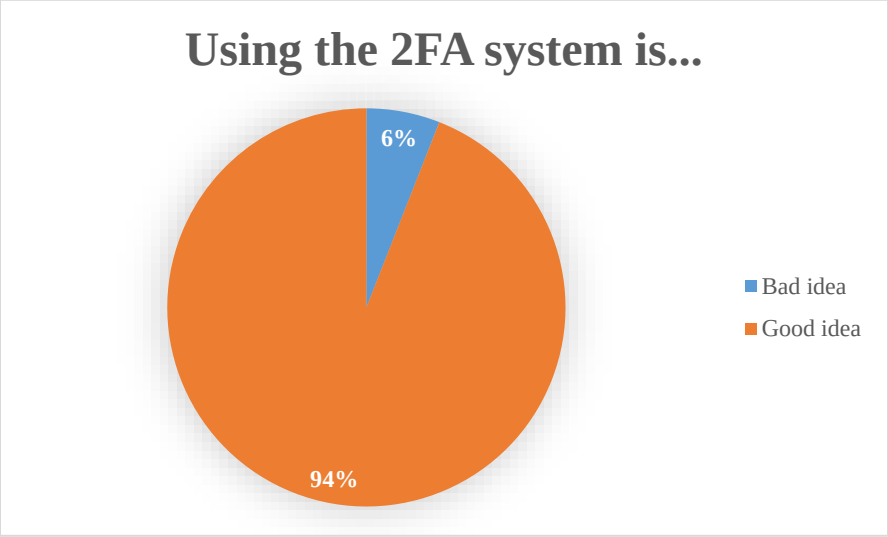
Source: Author's calculations, based on survey results

The importance of cybersecurity among TES employees



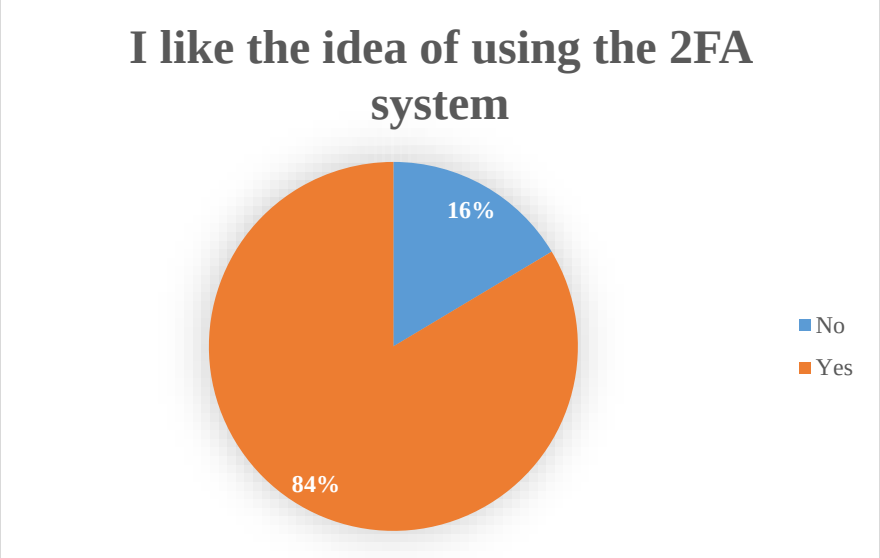
Source: Author's calculations, based on survey results

The opinion of TES employees in general of 2FA system



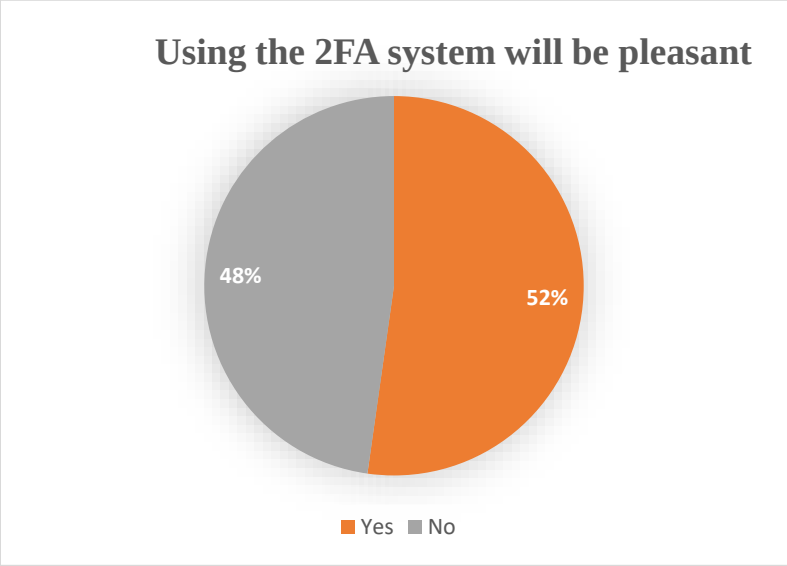
Source: Author's calculations, based on survey results

The preference of TES's employees



Source: Author's calculations, based on survey results

The system´s pleasure, author´s calculations



Source: Author’s calculations, based on survey results

Appendix 6. Questionnaire

Master´s thesis questionnaire research: Tallinn European School employees.

My name is Julija Mõnnakmäe, and I am currently doing my Master's thesis research in the Technology Governance and Digital Transformation program at Tallinn University of Technology. Iam conducting an analysis of technology acceptance among employees at the Tallinn European School. The questionnaire aims to find out people's opinions and attitudes toward the new digitalupgrade, such as "2-factor authentication" (2FA), in Tallinn European School (TES). The questionnaire consists of 16 questions and takes 3-5 minutes to complete. All responses will be anonymous, and no one will be identifiable in the research.

First, please read the explanation of 2FA and then answer the questions.

Two-factor authentication (2FA) is an identity and access management security method that requires two forms of identification to access resources and data. 2FA gives school the ability tomonitor and help safeguard our most vulnerable information and networks. Studies show that 2FA system reduces the amount of cyberattacks in organizations and makes the work environment more secure.

SMS verification or APP verification

SMS, or text messaging, can be used as two-factor authentication when a message is sent touser's phone number. The user is prompted to either interact with the text or use a one-timecode to verify their identity on a site or app.

How does it work?

Logging into your Microsoft 365 work account will immediately send a message to the phonenumber. You are prompted to use a one-time code to verify your identity on the site or app (Office).

The frequency of which users are prompted for 2FA depends on the organization's settings. Mostlikely, the system asks for identity confirmation when people sign in from a different device, change the location or password, so there is no need to verify your account each time you log in.The procedure in APP verification is similar, although the code for verifying your identity will appear on the app, which you should download before to your trustful electronical device.Please answer the questions from the perspective of cybersecurity.

General questions

1. Gender *

Please choose one

- ◯ Male
- ◯ Female
- ◯ Non-binary

2. Age *

Please choose one

- ◯ 20- 24
- ◯ 25-29
- ◯ 30- 34
- ◯ 35-39
- ◯ 40-44
- ◯ 45-49
- ◯ 50- 54
- ◯ 55-59
- ◯ 60-64

◯ 65-69

3. Nationality *

4. Do you have previous experience with a 2-factor authentication system? *

- ◯ Yes
- ◯ No

5. How important is cybersecurity in general to me? *
   Please choose one

- ◯ Extremely important
- ◯ Somewhat important
- ◯ Neutral
- ◯ Somewhat not important
- ◯ Extremely not important

Technology acceptance testing

6. Performance Expectancy *

Perceived Usefulness

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
Using the 2FA system would make me feel safe while using the work accounts.	○	○	○	○	○
Using the 2FA system will improve security of my organization.	○	○	○	○	○
Using the system in my job would increase the safety of the data I am working with.	○	○	○	○	○
I would find the 2FA system useful in my job.	○	○	○	○	○
I would feel less responsible for data leaks in my organization when using the 2FA system.	○	○	○	○	○

7. Effort expectancy *

Use of the system (Perceived ease of use)

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
Learning to use 2FA system would be easy for me.	○	○	○	○	○
I would have control over the system.	○	○	○	○	○
The use of the 2FA system would be clear and understandable for me.	○	○	○	○	○
It would be easy for me to become skillful at using the 2FA system.	○	○	○	○	○
I would find the 2FA system easy to use.	○	○	○	○	○

8. Social Influence *

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
If people who are important to me think that I should use the 2FA system, I will.	○	○	○	○	○
If people who are important to me think that I should not use the 2FA system, I will not.	○	○	○	○	○

7. Effort expectancy *

Use of the system (Perceived ease of use)

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
Learning to use 2FA system would be easy for me.	○	○	○	○	○
I would have control over the system.	○	○	○	○	○
The use of the 2FA system would be clear and understandable for me.	○	○	○	○	○
It would be easy for me to become skillful at using the 2FA system.	○	○	○	○	○
I would find the 2FA system easy to use.	○	○	○	○	○

8. Social Influence *

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
If people who are important to me think that I should use the 2FA system, I will.	○	○	○	○	○
If people who are important to me think that I should not use the 2FA system, I will not.	○	○	○	○	○

9. Facilitating conditions *

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
I have control over using the 2FA system.	○	○	○	○	○
I have the necessary devices to use the 2FA system.	○	○	○	○	○
I am aware of the opportunities 2FA provides and have knowledge about the use of the 2FA system.	○	○	○	○	○
The 2FA system is not compatible with other systems I use (in context of cybersecurity) .	○	○	○	○	○
If I need help using the 2FA system, I will have support and assistance in my organization.	○	○	○	○	○

10. Using the 2FA system is... *

(Attitude Toward Using Technology)

- ◯ Good idea
- ◯ Bad idea

11. Using the 2FA system is... *

Choose one

- ◯ foolish
- ◯ wise

12. I like the idea of using the 2FA system *

Choose one

- ◯ Yes
- ◯ No

13. I dislike the idea of using the 2 FA system *

- ◯ Yes
- ◯ No

14. Using the 2FA system will be pleasant *

- ○ Yes
- ○ No

15. Using the 2FA system will be unpleasant *

- ○ Yes
- ○ No

16. Comments

Please add comments (concerns, ideas)

Source: Microsoft Forms, Questionnaire conducted by author, based on the theoretical framework

Appendix 7. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Julija Mõnnakmäe (*author's name*)

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis

The analysis of attitude and motivation in implementing and adopting new digital update among employees of Tallinn European School,
(*title of the graduation thesis*)

supervised by Egert Juuse
(*supervisor's name*)

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

14.05.2023(date)

[1] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period*