

Caroline Stensland Selte

# How Moving from Traditional Signature Analysis to Automatic Anomaly Analysis Affects User Experience and Security Awareness

Master's thesis in Communication Technology

Supervisor: Maria Bartnes, Stig Henning Verpe, Roy Thomas Selbæk Myhre

June 2020



Caroline Stensland Selte

# **How Moving from Traditional Signature Analysis to Automatic Anomaly Analysis Affects User Experience and Security Awareness**

Master's thesis in Communication Technology

Supervisor: Maria Bartnes, Stig Henning Verpe, Roy Thomas Selbæk Myhre

June 2020

Norwegian University of Science and Technology

Faculty of Information Technology and Electrical Engineering

Dept. of Information Security and Communication Technology



Norwegian University of  
Science and Technology



**Title:** How moving from traditional signature analysis to automatic anomaly analysis affects user experience and security awareness

**Student:** Caroline Stensland Selte

**Problem description:**

All organizations are possible targets for cyber attacks, and attackers can take advantage of an organization's employees or partners to get access to the organization. For the organization, this can lead to severe consequences, so it is necessary to implement mechanisms to try to avoid these scenarios. In a security context, it is often stated that humans are the weakest link. Therefore technological security solutions are not enough just by themselves, there is also a need for making employees security aware by training. With the use of social engineering directed against employees, one way into an organization for people with malicious intentions is through electronic mail. As a part of the technological transformation in this century, the use of email has increased enormously and is a big part of an employee's everyday life. This development also increases the threat that email constitutes to the organization, because attackers can take several actions to exploit the frequent use and vast amounts of legitimate email.

Security monitoring is one of several technical actions that are taken in organizations today to ensure security for their systems, values and employees. Security monitoring has traditionally been rule based, but now new technologies are used to improve the security systems. The goal of this is better security by detecting attacks earlier and also by completely avoiding more attacks. Instead of defining all possible attacks in advance, machine learning algorithms that recognize abnormal behavior are able to detect attacks that have never been seen before. The abnormal behavior can be a sign of malicious actions, which further can lead to the detection of an attacker trying to compromise a system, malicious emails or other unwanted activities. For security solutions for email, advanced analysis of links and attachments can help detect malicious emails. The intention is to help the user understand what is insecure to open, and in this way avoid that malicious activity succeeds.

Even though the technology is changing, the users are still the same, and the human factor is still an issue. Therefore it is essential to investigate how technological changes are affecting the system users, and the master thesis is exploring this. The user experience will change because what the user is presented to will be different, including possible threats. How the change in user experience is affecting the users' security awareness and risk perception are important factors because these are

parameters that need to be understood to get a complete picture of the security context in an organization. For email solutions, a new representation of analyzed links and attachments is trying to give better decision support to the user and can lead to a different user experience and change in security awareness. The user may trust the analysis so much that they don't bother being critical to what they open, or maybe the advanced systems make the user more critical.

The primary purpose of the master thesis is to understand how the new email security solutions actually affect employees' risk perception, security awareness, perception of privacy and user experience, and further how this affects the security context in an organization. A big part of the master thesis is a case study of a knowledge organization, where we look into their security context, email solution and employees' security awareness. For this study, a mixed research methodology is applied, including semi-structured interviews with employees in the case organization. The goal is for this study to be a contribution to the development of security awareness training, and also to discover possible new threats that have evolved with the new solutions.

**Responsible professor:** Maria Bartnes, IIK  
**Supervisor:** Stig Henning Verpe, SINTEF  
**Supervisor:** Roy Thomas Selbæk Myhre, TietoEvry

## Abstract

There is now an ongoing transition in the field of security systems from traditional signature analysis to analysis using machine learning algorithms. Email solutions are among the systems that utilize this new technology. It is needed because email is a widely used attack vector for malicious activities, and it is possible to detect new kinds of attacks and avoid more attacks by utilizing machine learning algorithms. At the same time, new systems lead to a new user experience, but there is a lack of research on how changes in user experience affect security. This research project aims to fill this gap by investigating how this technological transition affects user experience and security awareness, with the ultimate objective of getting to know if organizations implementing these systems are becoming more secure.

A case study of a knowledge organization is performed to investigate how its employees are affected. Data was collected through semi-structured interviews with seven employees, analysis of emails reported as malicious and conversations with the IT security manager. The case organization is chosen because they, in fall 2019, implemented a new email security solution that utilizes machine learning algorithms.

Among the results are that the employees' risk perception is of a high degree and they have a good understanding of the potential email threats they and the organization are exposed to. There are internal differences, but in general, the new solution is well received among the employees and it seems like their user experience is slightly increased. Regarding security awareness, the results provide both factors that increase awareness and other factors that decrease awareness.

All the findings together imply that the total security is increased in the case organization after implementing the new security solution for email. The security is not perfect, and there is still room for improvements to the system. For improved security, the key message to organizations planning to introduce similar systems is to ensure that the employees have sufficient knowledge to utilize the systems correctly. For the users, it is important to remember that even though there are new and improved systems, they can never completely trust a system, so their human filter has to remain.





## Sammendrag

Tradisjonelt har sikkerhetsmonitorering vært regelbasert, men når blir det tatt i bruk maskinlæringsteknologi for å forbedre sikkerhetssystemene. E-postløsninger er blant systemene som bruker den nye teknologien. Dette er nødvendig fordi e-post er en av de meste brukte kanalene for ondsinnede handlinger, og det er mulig å oppdage nye typer angrep og unngå flere angrep ved å bruke maskinlæringsalgoritmer. Samtidige gir nye systemer en ny brukeropplevelse, men det mangler forskning på hvordan denne endringen i brukeropplevelse påvirker sikkerhetsbevisstheten til brukerne. Dette forskningsprosjektet prøver å fylle dette hullet ved å undersøke hvordan denne teknologiske endringen påvirker brukeropplevelse og sikkerhetsbevisstheten, men det endelige målet om å få kunnskap om organisasjoner som implementerer de nye systemene blir sikrere.

Et case-studie av en kunnskapsorganisasjon har blitt gjennomført for å undersøke hvordan deres ansatte blir påvirket. Data ble samlet gjennom semi-strukturerte intervjuer med syv ansatte, analyser av e-post som er rapportert som ondsinnet and samtaler med IT-sikkerhetsleder. Organisasjonen vi studerte ble valgt fordi de høsten 2019 implementerte et nytt sikkerhetssystem for e-post som baserer seg på maskinlæringsteknologi.

Blant resultatene er det at de ansatte har høy grad av risikopersepsjon og en god forståelse for potensielle trusler de og organisasjonen er utsatt for på e-post. Det er interne forskjeller, men generelt er den nye løsningen tatt godt imot av de ansatte og det virker som at brukeropplevelsen er noe økt. Angående sikkerhetsbevissthet viser resultatene både faktorer som øker bevisstheten og samtidig andre faktorer som minsker bevisstheten.

Alle funnene tilsammen gir indikasjoner på økt total sikkerhet i case-organisasjonen etter å ha implementert den nye sikkerhetsløsningen på e-post. Sikkerheten er ikke perfekt, og det er rom for forbedringer. For økt sikkerhet er hovedbudskapet til organisasjoner som planlegger å implementere lignende løsninger å sikre at de ansatte har tilstrekkelig kunnskap til å bruke systemene riktig. For brukerne er det viktig å huske at selv om det er nye og bedre systemer, kan de aldri stole helt på et system, så det menneskelige filteret må fortsatt være oppe.



## Preface

This master thesis is written to fulfill the MSc degree in Communication Technology at the Norwegian University of Science and Technology (NTNU). The work has been performed between January and June 2020 and follows the work with a pre-project fall 2019.

I would like to thank my supervisors, Maria, Stig and Roy. They have been very helpful and committed to the project, and I have learned a lot from them. I appreciate them taking their time to supervise me in the work with this project. I am also grateful to the ones who took their time to participate in the interviews. Finally, I would like to thank my family, friends and boyfriend for their support throughout this process.

Caroline Stensland Selte  
Trondheim, June 2020



# Contents

<b>List of Figures</b>	<b>xi</b>
<b>List of Tables</b>	<b>xiii</b>
<b>List of Acronyms</b>	<b>xv</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Motivation . . . . .	2
1.2 Limitation of project scope . . . . .	3
1.3 Research question . . . . .	4
1.4 Outline . . . . .	4
<b>2 Background and Related Work</b>	<b>7</b>
2.1 Email threats . . . . .	7
2.2 Threat prevention and security measures . . . . .	11
2.2.1 Security effects of automation . . . . .	12
2.3 User experience . . . . .	13
2.3.1 Usability . . . . .	13
2.3.2 Privacy and trust . . . . .	14
2.4 Human factors and people’s ability to change . . . . .	15
<b>3 Methodology</b>	<b>19</b>
3.1 Overview of the research design . . . . .	20
3.2 Data collection . . . . .	21
3.3 Literature review . . . . .	23
3.4 Conversations with the security manager in the case organization . . . . .	25
3.5 Data from reported emails . . . . .	25
3.6 Semi-structured interviews . . . . .	26
3.6.1 Recruitment of interview objects . . . . .	27
3.6.2 Structure and content of the interviews . . . . .	28
3.6.3 The conduction of the interviews . . . . .	29
3.7 Data analysis . . . . .	30
3.7.1 Qualitative analysis of interview data . . . . .	30

3.7.2	Analysis of reported emails . . . . .	30
3.7.3	Analysis of conversations with the security manager . . . . .	31
3.8	Case context . . . . .	32
3.9	Ethical considerations and privacy concerns . . . . .	33
<b>4</b>	<b>Results</b>	<b>35</b>
4.1	Information from conversations with the security manager in the case organization . . . . .	35
4.1.1	Results from a phishing campaign . . . . .	35
4.1.2	The new security solution . . . . .	37
4.2	Findings in the reported emails . . . . .	40
4.3	Interview findings . . . . .	40
4.3.1	Security awareness . . . . .	41
4.3.2	User experience . . . . .	45
4.3.3	Suggestions for improvement . . . . .	50
4.3.4	Analysis of reported emails . . . . .	51
<b>5</b>	<b>Discussion</b>	<b>61</b>
5.1	SQ1: How is the user experience intended to change with the new security solutions and how is the users' actual experience? . . . . .	62
5.1.1	Intentions of implementing a new security system . . . . .	62
5.1.2	Actual user experience . . . . .	63
5.1.3	Perceptions of protection of privacy and trust in the solution . . . . .	65
5.2	SQ2: How does this new user experience affect the users' security awareness? . . . . .	67
5.2.1	The employees' perception of risks and threats . . . . .	68
5.2.2	How the employees avoid email threats . . . . .	68
5.2.3	Are their behavior consistent with what they say? . . . . .	70
5.2.4	Effects on security awareness . . . . .	71
5.3	Implications . . . . .	73
5.3.1	Is the organization more secure now? . . . . .	73
5.3.2	Suggestions for improving the security solution . . . . .	75
5.4	Quality and limitations of the research . . . . .	76
5.5	Further work . . . . .	78
<b>6</b>	<b>Conclusion</b>	<b>81</b>
	<b>References</b>	<b>83</b>
	<b>Appendices</b>	
<b>A</b>	<b>Information to interview participants</b>	<b>89</b>
<b>B</b>	<b>Information to all emmploees in the case organization</b>	<b>93</b>

<b>C Interview guide</b>	<b>97</b>
<b>D Research approval from NSD</b>	<b>105</b>





# List of Figures

1.1	Relation between technological change in email security solutions, human factors and security culture. . . . .	3
2.1	Example of phishing email. . . . .	9
2.2	Overview of threats relevant to the objective of this master thesis. . . .	10
3.1	Necessary steps of understanding to answer the research question. . . .	20
3.2	Framework for research design by Robson [Rob11]. . . . .	20
3.3	Data sources in this research project. . . . .	21
3.4	The phases in the conducted literature review, inspired by Cronin et al. [CRC08]. . . . .	24
3.5	Tjora'a suggestion to the structure of an interview [Tjo10]. . . . .	28
3.6	Overview of themes and codes used in the analysis of the interviews. . .	31
4.1	Results 24 hours after phishing email was sent fall 2019. The vertical axis representing the number of employees out of 2000. Figure from pre-project report [Sel19]. . . . .	36
4.2	Results seven days after phishing email was sent fall 2019. The vertical axis representing the number of employees out of 2000. Figure from pre-project report [Sel19]. . . . .	36
4.3	Example of the graph presentation of an incident in the SIEM solution implemented in the case organization. Each node can be clicked for more information about the specific action. . . . .	37
4.4	Graph from the case organization's SIEM solution showing statistics on blocked URLs between February and May 2020. . . . .	38
4.5	Example of the change in presentation of URLs with the new email security solution in the case organization. . . . .	39
4.6	Example of spam email from the inbox with reported emails. . . . .	40
4.7	Example of phishing email from the inbox with reported emails. . . . .	41
4.8	Email number 1 of the analysis of reported emails during the interviews. Received before implementation of the new security functions. . . . .	52

4.9	Email number 2 of the analysis of reported emails during the interviews. Received after implementation of the new security functions. . . . .	53
4.10	Email number 3 of the analysis of reported emails during the interviews. Received after implementation of the new security functions. . . . .	54
4.11	Email number 4 of the analysis of reported emails during the interviews. Received after implementation of the new security functions. . . . .	55
4.12	Email number 5 of the analysis of reported emails during the interviews. Received before implementation of the new security functions. . . . .	56
4.13	Email number 6 of the analysis of reported emails during the interviews. Received before implementation of the new security functions. . . . .	57
4.14	Email number 7 of the analysis of reported emails during the interviews. Received after implementation of the new security functions. . . . .	58
4.15	Email number 8 of the analysis of reported emails during the interviews. Received before implementation of the new security functions. . . . .	58
4.16	Email number 9 of the analysis of reported emails during the interviews. Received before implementation of the new security functions. . . . .	60
4.17	Email number 10 of the analysis of reported emails during the interviews. Received after implementation of the new security functions. . . . .	60

# List of Tables

2.1	Criteria for HCI-S [JEL03]. . . . .	14
-----	-------------------------------------	----



# List of Acronyms

**ATP** Advanced Threat Protection.

**ENISA** European Union Agency for Cybersecurity.

**HCI** Human Computer Interaction.

**IDS** Intrusion Detection System.

**ISO** the International Organization for Standardization.

**ISP** Information Security Policy.

**IT** Information Technology.

**NorSIS** the Norwegian Center for Information Security.

**NSM** Network Security Monitoring.

**PST** the Norwegian Police Security Service.

**SIEM** Security Information and Event Management.

**SQ** sub-question.

**STS** Socio-Technical System.

**URL** Uniform Resource Locator.

**VPN** Virtual Private Network.

**ZTM** Zero Trust Model.



# Chapter 1

## Introduction

In the field of information security the technological development is significant. Right now, there is an ongoing transition from traditional signature based security monitoring to security monitoring using advanced machine learning algorithms. This transition is necessary because the organizations are broadening their attack surface as a consequence of the continuous digitization. Therefore, new security solutions are introduced to decrease the possibility of successful attacks in this situation. The new security solutions should be able to avoid more attacks and detect the attacks earlier to decrease the possibility of a successful attack. In addition to correct algorithms, the solutions also have to provide a good user experience that helps increase the security awareness of the user. A pleasant user experience is valuable because people's behavior is also essential to decrease the possibility of attacks.

Security solutions for email are among the new security systems. These are important because email is a widely used channel for attackers who want to spread their attack [Sym19][PST20]. People with malicious intentions can use email to send malware or to trick users into giving away personal information. There is always a human factor involved with email because there are people that decide which way to interact with the content if not stopped by the technological filters.

The need for improved security solutions comes from the digitization. Organizations today are more digitized than ever before, for example in the way that all systems are online, more devices are connected to the network and data are stored in clouds. More data is generated and stored about the organizations and their employees in this situation. This contributes to a broadened attack surface and organizations that are more vulnerable to cyber attacks. Risks increase as a consequence of the increased likelihood of attack and the worst-case consequences becoming more severe. The digitizing gives new opportunities but also new vulnerabilities, which further leads to new security challenges [Nas19]. The vulnerabilities can give major consequences, including monetary damage, corporate liability, and loss of credibility [BCB10]. In addition to threats targeted directly against an organization, the

organizations is also more exposed to vulnerabilities introduced through third-party organizations with possibly weaker security solutions [Nor20].

An example of how vulnerable an organization is to threats through the use of email, and therefore an example of the need for always improved security solutions, is the cyber attack targeted against Hydro in March 2019. Hydro was attacked and their IT systems were disturbed, resulting in that their operations were taken down and they had to operate manually [Hyd19]. These are severe consequences resulting from more functions being digitized and vulnerable in a new way. The attack was executed through a Trojan horse, which was attached to a legitimate email conversation with a customer of Hydro [ML19].

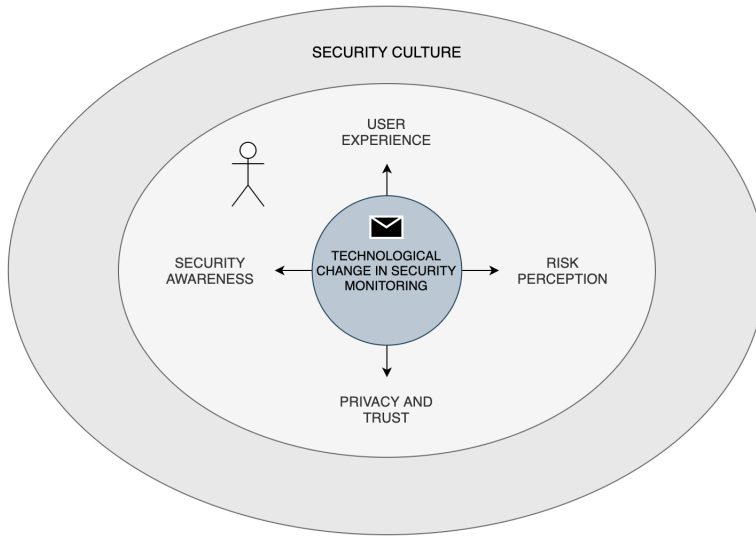
## 1.1 Motivation

Figure 1.1 illustrates that this technological change also has a human perspective that is very important and interesting. The user experience is changed when the system is changed. Further, the change in user experience can affect the security awareness of the users and their risk perception. Whether they perceive their privacy as protected or not, and if they have trust in the systems, are also factors influencing the user experience. With the new security monitoring systems using big data and machine learning, one example of a change the user might face is during an authentication process. A risk rate calculated from several parameters, for instance place and time, is used to decide whether two-factor authentication is necessary for the current situation. For this to be possible, the algorithms need large amounts of data about the user.

It is essential to understand how the user is affected by this change, because it is often stated that people are the weakest link in a security context. Even though the technology behind the solutions is becoming better, it is still the same people, with the same prerequisites, that are using the systems. Therefore, one motivation behind this study is to investigate the human perspective of this technological change. How can new technology change how threats are displayed to the user, and can some threats be removed? Are the users' guards lowered as a consequence of new security systems, or do the new presentations make the user perceive and understand risk in a new and better way? These are questions that we hope to find the answers to through this thesis.

The overall motivation for this study is to improve information security in organizations. A lot of time and money is spent on having the best available security systems, and the new technology is utilized to improve. It is interesting to look at how much factors like user experience and security awareness affect the security context in an organization, and how significant this human impact is, compared to





**Figure 1.1:** Relation between technological change in email security solutions, human factors and security culture.

the new technology. Knowing this can improve security because to improve, it is essential to know the weaknesses.

There is much research on new technology to improve the systems, but there is still missing information about how the users are affected. It is challenging to measure a change in users, but investigating this change is a motivation for this research project. The research is needed because there is a lack of research on how a change in user experience can affect security awareness, how human factors affect the new email solutions and privacy and trust in email security solutions.

## 1.2 Limitation of project scope

The transition to the use of machine learning in security monitoring is happening for many different types of solutions, but the project scope is limited to looking at email solutions. To look at and analyze all security solutions are too complicated for the master thesis work, and therefore the scope is narrowed down. There are also significant differences in the use of the systems, so a general analysis would not be satisfying.

The focus is email solutions because the solutions are used by employees every day and malicious emails are a significant security problem [Sym19] [Nor20]. People with malicious intentions use email to spread malware and send phishing emails or

spam. A threat report from 2019 shows that in Norway, 1 in 190 emails are malicious and the malicious Uniform Resource Locator (URL) rate is 12.8% [Sym19]. Another threat report shows that email delivers 94% of the total amount of malware [Ver19]. Further, 56% of Norwegian companies have been attacked or experienced an attempt through malicious emails [Nor20]. These numbers show that the threats coming from email are necessary to handle, and one solution is to use machine learning algorithms.

### 1.3 Research question

The objective of this study is to evaluate how organizations implementing these new systems change their total security and their employees' user experience and security awareness. The goal is to identify potential weaknesses that can be used for further improvement of security in organizations. A research question is created with two supporting sub-questions (SQs) to cover the whole scope of the research question and illuminate essential parts. The research question from the pre-project is almost maintained the same [Sel19]. The study will address the following research question:

**Research question:** How are the user experience and the users' security awareness affected when security solutions for email develop from traditional signature analysis to automatic analysis based on machine learning algorithms?

- **SQ1:** How is the user experience intended to change with the new security solutions and how is the users' actual experience?
- **SQ2:** How does this new user experience affect the users' security awareness?

The answer to this research question is a contribution to the academic community's field of user experience and security. There is little prior research on how a change in user experience and implementation of new systems affect security awareness, so this research project aims at filling this gap and provides a new perspective. When in possession of this knowledge, it can be used to develop security awareness programs for increased security. Further, it can be used by organizations to assess where to invest their money for increased security, how much is it worth spending on new solutions and how much should be spent on security training for employees. Hopefully, this thesis can also be an inspiration for further investigating issues in user experience and security, especially regarding new solutions based on new technology.

### 1.4 Outline

The structure of the thesis are the following:

**Chapter 1 Introduction:** Presents the topic of the thesis and the problem that is investigated through the research. The limitations of the project are defined and from that a project scope is established. Finally, the research question for the project is presented.

**Chapter 2 Background and Related work:** Includes relevant background information about the threat landscape and security measures. Then a presentation of related work to support this research project and to identify the lack of research that this thesis aims at filling.

**Chapter 3 Methodology:** Contains information about the research design with the methods used for data collection and data analysis. The case organization and some ethical considerations are introduced .

**Chapter 4 Results:** Presents the results obtained through the different methods for data collection.

**Chapter 5 Discussion:** Provides a discussion around the obtained results and relate them to previous research.

**Chapter 6 Conclusion:** Answers the research question and concludes the research.



# Chapter 2

## Background and Related Work

This chapter presents the information obtained from a literature review. It includes the necessary background information and interesting related work. First, the relevant threat landscape with main focus on the insider threat and email threats is presented in section 2.1. Then relevant measures against these threats are presented in section 2.2. In section 2.3, user experience is defined, and relevant studies are presented. Lastly, human perspectives are considered by the ability to change and the effects of and on risk perception and security awareness in section 2.4. Some of the presented information is background information used for the understanding of the context around the research, and some are related work that is directly attached to the research performed in this project.

### 2.1 Email threats

Email is a commonly used channel for delivering attacks, and therefore the use of email can be a huge threat to organizations. In Norway 1 in 190 emails are malicious and the malicious email URL rate is 12.8 % [Sym19]. The Norwegian Police Security Service (PST)<sup>1</sup> also highlights the email threat as a way to take advantage of human mistakes in Norwegian organizations, using directed emails with attached malware [PST20]. A common denominator for many email threats is that they are based on social engineering, trying to trick the user. Both sending phishing emails and emails with attached malware often utilize social engineering. In addition to the use of social engineering, malicious emails often contain a malicious attachment or malicious URLs. Four specific email threats are malware, ransomware, phishing and spam:

**Malware** is code that performs malicious activity on a victim's device. Email is the primary attack vector for malware [ENI19b]. Attackers attach malware to an email and send it to the victims, hoping that the receiver will open the attachment.

---

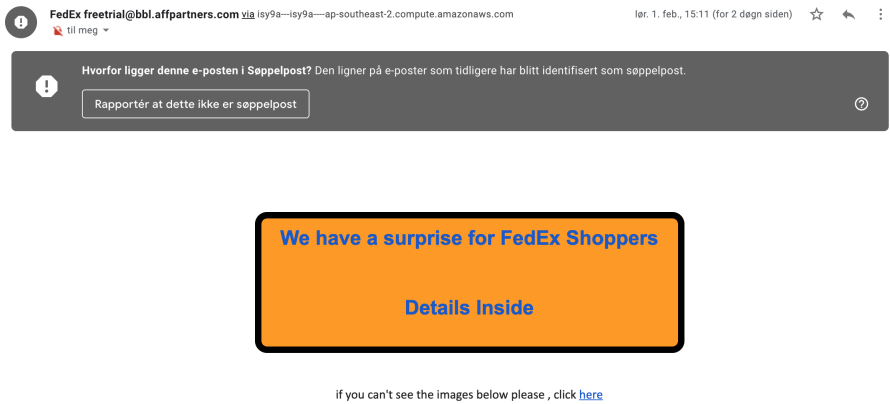
<sup>1</sup><https://www.pst.no/>

The email can also contain a malicious URL leading to a website with the purpose of making the victim download malware [ENI19b]. The malware can be something that will give the attacker control over the victim's computer, for example, spyware, viruses or worms. The attacker can use this to escalate their privileges, get sensitive information or other malicious actions [TJSB07]. If one employee's device in an organization gets infected, this can be damaging for the whole organization. To avoid opening malicious attachments, the user has to be aware of the risk, because the attachment often has regular file endings. Reports from both Symantec [Sym19] and Verizon [Ver19] shows that office files are the most usual kind of malicious attachment that brings malware.

**Ransomware** attacks are when an attacker gets control of files or devices and requires money to return the ownership. This loss of control has financial consequences but can also lead to a loss of credibility for the victim. According to European Union Agency for Cybersecurity (ENISA) the use of ransomware is decreasing and mostly being replaced by cryptojacking, but in 2018 3.2% of security breach incidents still was because of ransomware attacks [ENI19b]. At the same time the Norwegian Center for Information Security (NorSIS) is reporting an increase in ransomware attacks in 2019 [Nor20]. Ransomware is an email threat because in 2018 65% of all ransomware attacks were delivered through email [ENI19b].

**Phishing** is the use of crafted messages using social engineering techniques to trick a receiver. They can, among other things, lead the victim to open malicious attachments, click on unsafe URLs and hand over their credentials. The phishing messages are often sent as emails [ENI19b]. An example is shown in figure 2.1 where the sender is pretending to be a well-known enterprise, saying that they have a surprise for the receiver if the receiver proceeds by clicking a link. If the link is clicked, the receiver will typically have to give away personal information, like login credentials or credit card data. The attacker steals this information and there is no real surprise for the receiver. Phishing emails like this can often be recognized by lousy language, unconventional sender email addresses and offers that are too good to be true. The threat landscape report by ENISA from 2018 shows that phishing is the biggest weakness in the case of the unintentional insider threat. It also lists the most commonly seen words in malicious emails during 2017 as *delivery, mail, message, sender, your, returning, failed, invoice, images and scanned* [ENI19b].

**Spam** is to flood users with unsolicited messages, often via email. It is a threat because of its opportunity to be sent in huge volumes and take up bandwidth and storage capacity. Besides that, it can contain malicious URLs and attachments. Even though the spam levels are lowered the last years, it is still considered a relevant threat [ENI19b].



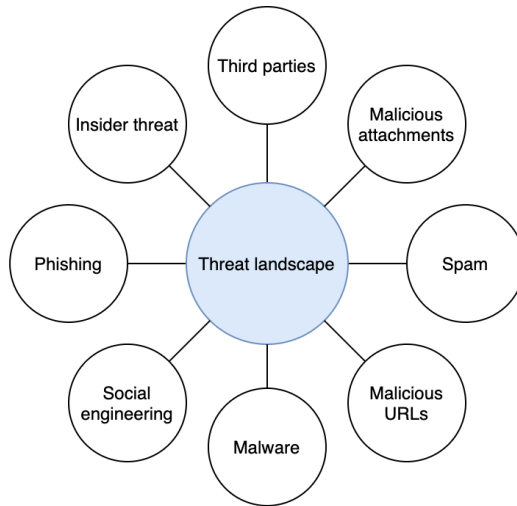
**Figure 2.1:** Example of phishing email.

An attack can lead to compromise of the employees' device or release of sensitive information [TJSB07]. Therefore, malicious emails are a significant threat if there are no security systems that help the user understand which emails are malicious and which emails are safe. Even though security systems are implemented, there is no guarantee that all malicious emails are detected. Attackers are creative and will always come up with new ideas to trick the receivers. In this way, there is a forever ongoing arms race between security developers and hackers.

As figure 2.2 shows, a big part of the relevant threat landscape for the objective of this master thesis is email threats, but the insider threat is also significant because the humans are often considered the weakest link in a security context. The link between email threats and the insider threat is strong because malicious emails are often utilizing social engineering, which can increase the unintentional insider threat. It is also linked the other way because the existence of the insider threat is increasing the possibility of succeeding with attacks through email.

To be an insider threat, a person has to currently have or previously have had authorized access to the organization's network, system or data, and used it intentionally or unintentionally in a manner that negatively affects the organization. To use it negatively means destroying the confidentiality, integrity, availability or physical well-being of the organization's information, systems or workforce [TTC<sup>+</sup>19]. There are several risks that contribute to increasing the risk of the insider threat. The Norwegian National Security Authority's<sup>2</sup> risk report of 2019 [Nas19] presents six main risk factors in Norway, where several of them emphasize the risk of not having secured the organization's systems and information good enough and having

<sup>2</sup><https://www.nsm.stat.no/om-nsm/>



**Figure 2.2:** Overview of threats relevant to the objective of this master thesis.

weak security management. Organizations without access control, segregation of the networks and logging are more vulnerable to the insider threat [Nas19]. The insider threat exists because an employee in an organization has access to the entire network and privileges in the system, and can potentially do much damage without being revealed. The threat landscape report by ENISA from 2019 [ENI19b] states that the primary reason that a company is vulnerable to the insider threat is the unreasonable access privileges given to many employees. This can, for example, be a problem if an employee that receives a malicious email gives away their credentials to a person with malicious intentions, who then will have all the privileges that the victim has. The damage will be unnecessarily big if the victim has unnecessary privileges, which gives the attacker greater access and information.

The report about threats and trends by NorSIS [Nor20] shows that social manipulation and targeted, personalized attacks will most likely become more common. One reason for this is that when technology is becoming better, it is easier for the attackers to take advantage of humans instead of cracking the technology. In addition, the machine learning technology together with the enormous amounts of data that now exist makes it easier for the attackers to create good phishing emails with personal data about the receiver [Nor20].



## 2.2 Threat prevention and security measures

Because of the complex threat landscape, security measures are necessary to protect an organization and decrease the vulnerabilities. The security measures can be both technical and human, and the interaction between those is of interest. How the technical measures are affected by how people are using them is an important aspect to understand the security effect of the measure.

The first important measure for increased security is to ensure that users are performing the right actions when using email, as far as that is possible to ensure. Email can be considered a Socio-Technical System (STS) because it is a widely used technical tool to provide communication, which is a necessary, societal function [Gee04]. The human interaction with the email security systems are crucial, and Geels [Gee04] states that the STSs do not function autonomously, but are the outcome of the activities of human actors. People in the STSs are always evolving and are not as predictable as the technology [FRS05], which is a reason to try to control the user's possibilities.

Flechais et al. [FRS05] define two fundamental properties for security countermeasures; correctness and dependability. Correctness in the way that the threat is neutralized by the countermeasure, and dependability means that the countermeasure is working as intended. The human factor can affect the dependability and make the system less dependable, as a consequence of being less predictable than technology. This possibility is why it is interesting to look at email as a socio-technical system where human factors affect security.

The Zero Trust Model (ZTM) is a model that can be used for threat prevention in an organization. The ZTM eliminates the idea that some networks are looked at as trusted, and instead, all networks are considered untrusted [Kin16]. From that, we eliminate the threat coming from looking at all insiders as trusted, and thereby decreases the insider threat. The ZTM includes to verify and secure all resources, limit and strictly enforce access control and inspect and log all network traffic [Kin16].

One way to inspect and log all network traffic is to use Network Security Monitoring (NSM), which is a necessary tool to protect an organization against threats. It is a broad term, and there are many definitions, but the essence is the same. Bejtlich [Bej04] defines NSM as: "The collection, analysis, and escalation of indications and warnings to detect and respond to intrusions." Here indications are the direct output from the system, and warnings are results of an analysis of indications performed by an analyst. The system is responsible for collecting data in the network, and people are performing the analysis. Escalation is the process where the information is given to the decision makers [Bej04].

Intrusion Detection Systems (IDSs) are systems used for monitoring to detect intrusions. IDSs can be classified into two different types, misuse detection systems and anomaly detection systems. Misuse detection systems monitor the network with knowledge of malicious behavior and compare network traffic with signatures describing attacks. Anomaly detection systems create profiles of normal behavior and alarms about abnormal behavior. Machine learning algorithms detect attacks by first learning normal behavior and then by being deployed on unseen data [SP10]. IDSs are mainly used to detect intrusions in a network or on a host machine, but can also be implemented for email clients. Email threat protection is a mechanism to provide security in the use of email systems. Traditionally this is done by using spam filters that filter out an unknown or suspicious email before it reaches the user's inbox. This filtering is functioning like an IDS.

Security Information and Event Management (SIEM) is another kind of monitoring tool that gathers data from different sources and performs analysis. In addition, it also manages the detected incidents by taking the appropriate actions. Sources the SIEM tool uses are, among other, IDSs, firewalls, end devices and network equipment [Rou20]. The modern SIEM tools are using machine learning algorithms, artificial intelligence and big data, and because of that, they continuously improve with use. For the system to fit perfectly to an organization, the operator can also optimize many different parameters [Rou20]. Especially regarding email solutions, these systems can analyze links and attachments, and thereby provide decision support to the user on what to trust.

### 2.2.1 Security effects of automation

The goal with security monitoring and automation of systems is obviously to increase security, but Edwards et al. [EPS08] write about the limitations in automating end-user security. Automation involves that the decision is completely removed from the user, so it is about an automatic response to intrusions. The automation removes the possibility of human errors, and at the same time, fully trust that the system does not make any mistakes. IDSs and SIEM solutions are not completely automated because there is also a human operator included in many decisions, but they still include an automatic analysis and an increased amount of automatic processes. Edwards et al. [EPS08] state that many users are more dedicated to their primary tasks than to security tasks and that users neglect to adapt to security measures. Therefore it is critical to understand the limitations of automation and take the non-technical constraints into account when working to improve security [EPS08]. *As Edwards et al. [EPS08] recommend, further research is needed on the more socially relevant form of security for end users. The research in this project will evaluate how the new security solutions for email takes the human aspect into account.*

## 2.3 User experience

In this project, there are two different aspects of user experience that are important. The first aspect is the change in the presentation of links and attachments. The change in presentation can change the usability of the system, and therefore affect how user's use the system in the way that the Human Computer Interaction (HCI) is changing. The second aspect is the possible change in people's trust and perception of protection of their privacy, which also are factors that can affect user experience.

The International Organization for Standardization (ISO) defines user experience in ISO 9241-11 [ISO18] as: "User's perceptions and responses that result from the use and/or anticipated use of a system, product or service." Responses and perceptions are about the user's emotions, beliefs, preferences, perceptions, comfort, behaviors and accomplishments that occur before, during and after use. User experience is a consequence of both the system's functionality, performance and characteristics, and the user's internal and physical state. The user's state is affected by prior experiences, skills, attitudes and personality in a user context [ISO18].

User experience as a research field started without any focus on security, but the focus on security has increased. This is important because a usable and a secure system is not always the same, and the lack of usability can turn a secure system into an insecure system. For example, in the way that bad usability can increase the unintentional insider threat. *Even though there is now research in the field of user experience and security, like [JEL03], there is a lack of research on how a change in user experience can affect the security. This research project aims at filling this gap.*

### 2.3.1 Usability

Usability is a characteristic of a system, and Nielsen [Nie93] associates it with learnability, efficiency, memorability, errors and satisfaction. To evaluate usability, heuristics can be used. Nielsen [Nie94] tested several sets of usability heuristics and created an ultimate list of ten heuristics. Out of the ten heuristics provided by Nielsen, there is not a single one that is focusing on security. To prevent errors is mentioned as a vital part of good usability, but only in the form of mistakes. One term that is later introduced is *HCI-S* [JEL03]. Johnston et al. [JEL03] have written a paper to promote and enable security awareness of end users in interaction with computer systems. They define HCI-S as: "The part of a user interface which is responsible for establishing the common ground between a user and the security features of a system. ..." [JEL03]. As presented in table 2.3.1 they also introduce a set of criteria, expanded and modified from Nielsen's criteria [Nie94], that can be used to create software that is both usable and secure. The ultimate goal is for the user to trust the system.

No.	Criteria	Description
1	Convey features	The interface needs to convey the available security features to the user.
2	Visibility of system status	It is important for the user to be able to observe the security status of the internal operations.
3	Learnability	The interface needs to be as non-threatening and easy to learn as possible.
4	Aesthetic and minimalist design	Only relevant security information should be displayed.
5	Errors	It is important for the error message to be detailed and to state, if necessary, where to obtain help.
6	Satisfaction	Does the interface aid the user in having a satisfactory experience with a system?

**Table 2.1:** Criteria for HCI-S [JEL03].

Jakobsson et al. [JTS<sup>+</sup>07] investigated which parameters that are affecting the trust people have in emails and web pages, and among other things found that the URL is an important factor. People suspects URLs that is IP addresses or syntactically different to be malicious. On the other hand, people were not suspicious about well-formed and simple URLs. *There is a need for updated research on this topic, and in this master thesis we will look into how long and complicated URLs are evaluated and which links the receiver finds suspicious.*

### 2.3.2 Privacy and trust

Another perspective of user experience is how the users perceive the protection of their privacy and if they feel that they can trust the system. The definition of user experience by ISO includes the user’s perception after use [ISO18], and privacy and trust are essential parts of this perception.

Privacy is the right to keep personal matters secret and to be let alone. Information privacy is the right to have control of your personal information, meaning how it is collected and used [IAP19]. For this research project, it is the information privacy and the perception a person has of whether their privacy is perceived or not that is relevant. The machine learning algorithms utilized in the analyzing systems need a lot of data for training and detection. The systems are complex, and not only for email. A central Advanced Threat Protection (ATP) gathers data from many different systems and learns a lot about the users and what they do. Privacy

preserving machine learning algorithms are used, but despite this, there will always be a probability that users feel that their privacy is not sufficiently protected. In some cases, this might also be true. If a user feels that their privacy is not protected, it can affect their user experience. Further, it might lead to the user utilizing the systems differently and changes the security parameters. These are actions that can lead to decreased security in an organization.

There is research on the effects that lack of privacy has on trust and therefore user experience. Seckler et al. [SHF<sup>+</sup>15] state that lack of privacy increases the distrust. Bart et al. [BSSU05] found that web sites with high information risk privacy have protection of privacy as one of the essential factors for trust. This shows the importance of good privacy for the user to trust the system, and that privacy and trust are tightly connected because privacy is a significant factor for online trust.

To create a good HCI, trust is very important [SHF<sup>+</sup>15]. Trust is defined in the Oxford English Dictionary as: "Firm belief in the reliability, truth, or ability of someone or something. ..." [oxf15]. In this context the something is an email security solution based on machine learning technology, and trust includes that the user can rely on the security provided by the solution. Most research on online trust is done in the field of e-commerce, but some of the results in this field can be transferred to other domains, like email security. The criteria presented in table 2.3.1 are also created to enhance trust because trust is important for a user to use the system to its full potential [JEL03]. Wang and Emurian [WE05] conclude among other things that even when an interface is created to induce trust, the consumer will still have to be informed about risks and protections that are present. This is a part of the criteria that Johnston et al. presented [JEL03].

*Even though some of the findings in the field of online trust regarding web pages and e-commerce can be transferred to email solutions, there is a lack of research directly on email security solutions. This research project aims at filling the gap of missing research on privacy and trust in email security solutions by looking at how these factors change with the new system.*

## 2.4 Human factors and people's ability to change

Human factors in the context of information security are important because humans are often considered the weakest link, and two essential factors are security awareness and risk perception. A big part of this research project is to understand how human factors are affecting the security in an organization after implementing new systems. An employee's risk perception and security awareness affect their actions and further the organization's security. Since the project is investigating a change, theory on people's ability to change is necessary to understand how security awareness and risk

perception is changed with the new technology. First, the terms security awareness and risk perception are defined:

**Risk perception** is about how people think about and respond to risk. People with knowledge about a topic perform risk assessment, but other people have an intuitive risk judgment, which is called risk perception. People's risk perception varies a lot, and different factors underlie the perceptions of risk. These factors can be both social and cultural [Slo87].

**Security awareness** is defined by Bulgurcu et al. [BCB10] as "an employee's overall knowledge and understanding of potential issues related to information security and their ramifications." The objective of creating security awareness involves making employees conscious of the risks related to information security and to instruct them about their responsibilities concerning those risks, with the goal of making them feel commitment [BCB10].

Bulgurcu et al. [BCB10] performed a study on which factors influence an employee in their commitment to the organization's Information Security Policy (ISP), so-called compliance behavior. There is no benefit in having an ISP if the employees do not see any reason to follow it, or they gain more if not following it [BCB10]. The same might count for new technological security solutions. For the organization to benefit from it, the employees need to be motivated and educated enough to use them correctly. The study by Bulgurcu et al. [BCB10] stresses the significant influence of security awareness on attitudes and shaping of outcome beliefs. Further, an employee's attitude, normative beliefs and self-efficacy have a significant impact on the intention of following the ISP [BCB10]. These factors are not directly the same as risk perception, but factors in the context of risk perception. The study illustrates the importance of employee's security awareness for the organization's information security.

ENISA published a report in 2019 [ENI19a] based on investigations they have done on existing literature about human aspects of cyber security. Such research on human behavior in meeting with computer systems is important since information security can be considered a socio-technical problem [ENI19a]. To understand how human behavior affects security in an organization, as well as their security culture, is a part of this. To influence the employees' security behavior will, in many cases, require a behavior change. The report reveals that to increase the users' understanding and fear for cyber incidents is not enough to change behavior. This might be because most people already have enough knowledge about cyber threats or do not have the necessary tools to cope with it anyway [ENI19a]. The report also concludes from the review that there is a link between the ability to cope in the face of threats and their cybersecurity behavior. To cope includes both to respond in a way that actually

works and the ability to respond. This means that increase in coping skills improves cybersecurity behavior. Another essential thing to note from the report is that behavioral change will only happen if the behavior is achievable in the employee's everyday activities [ENI19a]. The specific change studied in this master thesis is meant to help the user in making decisions, and should not be an obstacle in the everyday activities of an employee.

In 2016 NorSIS conducted a survey on factors that influence risk perception. It shows that most people think they are exposed to risk when they are online, and most think there is a larger threat that someone else will do something to you than that you do something by yourself that harms you. Further, it investigates the relation between recent cybersecurity education and perceived risk, and it shows that educating does not significantly change the perception of digital risk [MR16]. This complies with what ENISA found [ENI19a]. The article by NorSIS does not suggest other ways to increase risk perception. The finding by both NorSIS and ENISA is conflicting with a study from 1990, which enhances both the use of security software, focus on security and education to increase information systems security [Str90].

It is essential to understand how people think about and respond to risk so that security awareness training can be adapted. Much research conducts around this topic. At the same time, both [ENI19a] and [MR16] state that security education is not necessarily enough to increase the risk perception and improve security behavior. It is also vital that behavior changes take time, and cannot be expected to happen instantly [ENI19a]. *It is, therefore, a need to investigate other ways for increased security awareness and decrease in human errors. This research project looks into what happens to security awareness and risk perception when introducing new systems with new user experiences. It also investigates how human factors affect the new solution and security. A limitation is that change hard to measure because it takes time.*





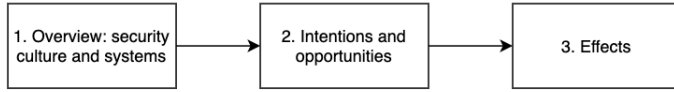
# Chapter 3

## Methodology

The research in this project is conducted through a mixed research methodology and is a case study of one organization. This chapter explains the applied methods and considers the advantages and disadvantages. Since the research looks into human factors and social aspects, the research methods used will be from the social science domain. The primary references are books by Aksel Tjora [Tjo10] and Colin Robson [Rob11]. First, an overview of the research design is given in section 3.1, before section 3.2 presents the choices of methods for data collection. The following four sections, 3.3, 3.4, 3.5 and 3.6, presents details around each data collection method. Then the methods for the analysis of the collected data are presented in section 3.7. Section 3.8 gives an introduction to the case organization and their security situation, and lastly section 3.9 presents the necessary ethical considerations.

An overall plan was created and presented in the pre-project report [Sel19] explaining the process to obtain the necessary data to answer the research question. Figure 3.1 presents the phases, and each phase involves to:

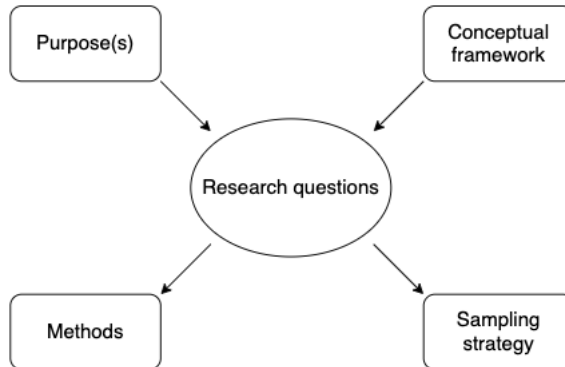
1. Get a good overview of the situation in the organization before implementing the new security solutions. The focus of this phase is the current security culture and the systems that are in use today.
2. Look at the case organization's intentions for the new solution's effect on the security context in their organization. Which opportunities do the new solutions provide to users and the organization, and how can this change the threat landscape.
3. Understand how the new solutions really affect the user's risk perception, security awareness and user experience, and further how this affects the security context in the organization.



**Figure 3.1:** Necessary steps of understanding to answer the research question.

### 3.1 Overview of the research design

Research design is the layout on how to conduct the research to get answers to identified problems, including methods and procedures. It can be fixed, meaning that the design is locked before the data collection takes place. It can also be flexible with the possibility of changes in the design during the research. A third possibility is a multi-strategy design, also known as mixed research methods, using both fixed and flexible design strategies [Rob11]. Robson [Rob11] presents a framework for research design, as presented in figure 3.2.



**Figure 3.2:** Framework for research design by Robson [Rob11].

For this research project, we have identified the following:

**The purpose** of the project is to understand how a technological change affects users of systems applying new technology from a security perspective. This knowledge can be used to learn about new threats and the necessary development of employees' security awareness training. The hope is that this can eventually lead to better information security in organizations.

**The conceptual framework** involves the human factors; user experience, security awareness and risk perception. The theory is that the technological change

affects these factors. Further, the question is how and to which degree it affects and what impacts these effects have on security culture.

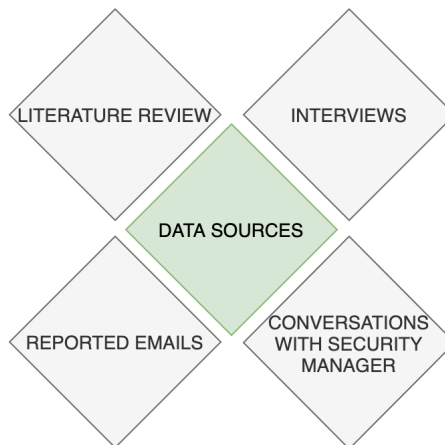
**A research question** is created to get the answers needed to achieve the purpose of the project, and it is: *How are the user experience and the users' security awareness affected when security solutions for email develop from traditional signature analysis to automatic analysis based on machine learning algorithms?*

**The sampling strategy** is to seek data from a case organization. The research is carried out as a case study, and all data is collected from one organization.

**Methods** are chosen to fulfill the purpose and answer the research question. It is chosen to use four different methods, including semi-structured interviews, a literature review, a collection of statistics from reported emails and conversations with the security manager in the case organization.

### 3.2 Data collection

Four different methods, as shown in fig 3.3, are utilized to collect data in this research project. The chosen methods are qualitative methods that aim at insight and are suitable to increase understanding of a problem. This is in contrast to quantitative methods that search for explanation and overview of a problem [Tjo10] [Rob11]. For this study, a combination of literature research and three qualitative research methods are used.



**Figure 3.3:** Data sources in this research project.

The use of several methods for data collection is the concept of methodological triangulation. Triangulation reduces the validity threat and tests the consistency of findings [Rob11]. The use of several methods allows the use of the data from one method to interpret data collected using a different method. This can increase the understanding of a problem and, therefore, give more validity and completeness to the final results. On the other hand, using several methods can be time-consuming, and it also requires skills and training. This research project is carried out in a short time frame and is a master thesis, but both these complexities are obstacles that are handled with proper preparation. Another complexity that might appear when using several methods is a lack of integration in findings [Rob11].

The four approaches are chosen because collectively they provide the data needed to answer the research question, and the chosen methods are:

- Semi-structured interviews with employees in the case organization, which are a qualitative method and will be the primary data source.
- Conversations with the security manager in the case organization.
- Collection of data from an inbox with emails that employees in the case organizations have reported.
- Literature review on previous research and relevant theory. Relevant documents include research papers, technical reports and books.

The primary data collection method is interviewing, but observations and a questionnaire were also considered as possible methods. Observations help find out what people do in public [Rob11]. It has the advantage of observing the employees in their natural environment and not allowing them to choose what to answer. However, it is not chosen because it will not give the necessary responses. For this research, the employees' attitudes, beliefs and behavior are of interest, and observation is not sufficient to get to know these parameters [Rob11]. A questionnaire is another suitable alternative to interviews. It has the benefit of being less work for the respondents, which probably can give answers from more employees and thereby give a more representative selection of the organization. On the other hand, a questionnaire requires perfectly formulated questions with no room for misunderstandings, and there is no possibility of asking follow-up questions to the informants. There is also only possible to get answers that were already thought of as alternatives [Tjo10]. To gain the necessary insight needed in this research, the use of follow-up questions is essential and also the possibility to get new perspectives from the participants, and therefore interviews are chosen. A combination of interviews and a questionnaire would probably be the best solution, but because of time limitations, only interviews are used.

The four following sections explain how the chosen data collection methods are used in this research, their advantages and disadvantages and the reason for choosing them for this project.

### 3.3 Literature review

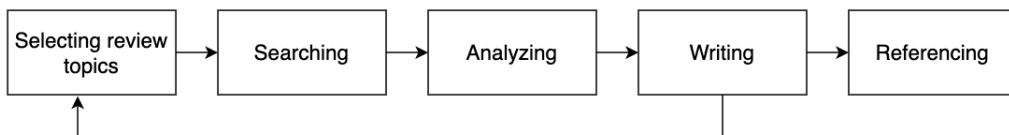
According to Hart [Har98], a literature review is the analysis, critical evaluation and synthesis of existing knowledge relevant to a research problem. It is the selection of available documents on the topic and evaluation of these. The literature review follows a literature search, where relevant papers and sources are found. A literature review is central in many research projects and is often used as a source for background information [Tjo10].

During the first part of the work with this master this we performed a literature review and the results are mainly presented in chapter 2. The goal of this literature review was to study previous research work, understand concepts and gain insight into the current threat landscape. One reason to do this is to justify the research topic, design and methodology [Har98]. It is also necessary with this insight and understanding before going into the interviews, and to be able to analyze the results. The use of this method is also unobtrusive and is, therefore, an appropriate alternative to reduce the load on the research participants [Tjo10]. However, most of the relevant literature is written for other purposes than our research, which is important to remember when performing the literature review.

A good literature review requires structure, both in the process and presentation [CRC08]. There are several suggestions to this process, and Cronin et al. [CRC08] suggest the following process for a literature review, which is similar to what Randolph [Ran09] presents:

1. Selecting a review topic
2. Searching the literature
3. Gathering, reading and analyzing the literature
4. Writing the review
5. References

The process presented in figure 3.4 is the process we followed in this research project's literature review. The first four phases were repeated because after analyzing a paper, the need for new literature arose. New knowledge gave way for new search



**Figure 3.4:** The phases in the conducted literature review, inspired by Cronin et al. [CRC08].

topics, and the rest of the process followed again. During the process, a reference list with all used papers where created. The phases mainly consisted of the following:

**1. Selecting a review topic:** It is essential to be specific in the selection of review topics, for the number of results to be manageable [CRC08]. For this research, it is interesting to collect knowledge about the research field and to investigate if anyone has tried to answer a similar research question earlier. To get the desired search results, the search words that were used are: *user experience, security awareness, risk perception, security monitoring, privacy, trust, threat landscape, email security, email threats, change in technology and machine learning*, and several combinations of these. In addition, we also searched for information about methodology and thesis writing.

**2. Searching the literature:** The search words are used to find relevant literature. In the beginning, the search was performed using Google Scholar<sup>1</sup>. Further, references in the papers were followed to discover new and relevant papers. Specially articles published on IEEE Xplore<sup>2</sup> and Science Direct<sup>3</sup> where used as resources, as these are peer-reviewed. To find reports on current threats, a standard search engine is applied. In addition, NTNU's library search Oria<sup>4</sup> is used to find relevant books on methodology.

**3. Gathering, reading and analyzing the literature:** The process of gathering literature by determining what is appropriate is a critical part [CRC08]. To first start reading the summary and conclusion, can tell if the article is worth spending more time on. Relevant articles are the ones that provide new and relevant information on the review topics directly or indirectly and can be qualitative or quantitative studies. The relevant articles are further read and analyzed. The most important findings were noted and categorized by topic.

<sup>1</sup><https://scholar.google.no/>

<sup>2</sup><https://ieeexplore.ieee.org>

<sup>3</sup><https://www.sciencedirect.com/>

<sup>4</sup><https://bibsys-almaprimo.hosted.exlibrisgroup.com/>

**4. Writing the review:** The review should be written in a clear and consistent way to present the findings [CRC08]. In this thesis, chapter 2 presents the findings as related work and background information.

**5. References:** The bibliography in this thesis includes all used references.

### 3.4 Conversations with the security manager in the case organization

Conversations with the case organization's security manager are used to understand the situation in the case organization before implementing new security solutions and looking at what intentions the organization has for the new solutions. To understand this is an essential part of the phases presented in figure 3.1. The conversations are not only focused on the email solution, but also on the complete security solution they have implemented that rely on big data and machine learning.

The conversations are focused around predefined topics but are not structured as an interview. For one of the conversations, it was prepared some questions to make sure everything necessary was covered. Therefore that conversation is more like a semi-structured interview. Nevertheless, the choice of using conversations as a method, which is quite informal, is taken because it has been close cooperation with the case organization during the entire project. To use a method that is not a standard method with many rules has both advantages and disadvantages. It is good because it is adapted to the exact research, but it might be harder to do the same later. The gathered information is mainly facts and not opinions, and therefore the information should be the same through the use of other similar methods.

Chapter 4 presents most of the data from the conversations. In addition, some of the gained knowledge is used in section 3.8 about the case context and generally as background information when writing this thesis.

### 3.5 Data from reported emails

The employees in the case organization have the possibility to report the emails they receive if they think there is something suspicious or that the email is spam. The security department added this function in November 2016. To report an email, the employee clicks a button in their inbox, and then the system forwards the email to a separate inbox that the Information Technology (IT) security staff can access. The intention with this is to get to know which emails that pass the security mechanisms and being able to alert other employees that might have received the same email. Another purpose is to lower the threshold for reporting security incidents and it is a vital human filter in addition to the spam filters.

Data explaining how the employees actually behave is found by looking at the emails they report. Looking at their behavior from before and after the technological change can give information about potential development in security awareness. This data are a great supplement to the data from the interviews where the employees are explaining how they experience the change. When creating the interview guide, the emails are also used by including ten of the reported emails in the interview.

A challenge with the use of these results is that many different factors affect what is reported so that a potential development might be because of other factors than a change in technology and user experience. Therefore it is necessary with several data sources, and the disadvantage is reduced because these data are mainly used to support other collected data.

### 3.6 Semi-structured interviews

Semi-structured interviews are also known as focus interviews and are the interview form used in this research project. Other interview alternatives are fully structured or unstructured. Semi-structured interviews follow an interview guide with topics to be covered and some questions in order, but with the possibilities of unplanned follow-up questions and following the flow of the conversation [Rob11]. Tjora [Tjo10] supports this by stating that semi-structured interviews intend to create a situation where there is space for relatively open dialogue around some predefined subjects.

The purpose of the interviews in this research project is to get to know how the employees look at threats, the possible consequences of their behavior and their responsibilities. This understanding gives insight into their risk perception and security awareness. We also try to understand how the user experience with the new solutions is and how they perceive the protection of their privacy and whether they have trust in the solution. To get the interviewee to reflect around these topics are essential, and semi-structured interviews are therefore suitable.

Another reason that semi-structured interviews are chosen is its flexibility and adaptability. Open questions allow the participants to elaborate on topics where they want to. It also has the advantage of the possibility to bring new ideas to the table that no one has thought about in advance of the interviews [Tjo10]. On the other hand, a fully structured interview requires all questions to be prepared in advance, and an unstructured interview would have the risk of not covering the information needed to answer the research questions. An advantage with interviews, in general, are the non-verbal cues that can help in interpreting the verbal responses, which will not be there in surveys and questionnaires [Rob11]. These clues are useful because they can give a more profound understanding, as they make the information more complete. It also can help in interpreting whether the responses are honest or not.



The main disadvantage of interviews is the time consumption. Preparation, subscription and analyzes are all part of the interview process that are time consuming for the researcher. Therefore the number of interviews is limited to seven in this research. It is also a method that asks a lot from the participants because an interview often requires more time than, for example, to answer a questionnaire. This can lead to a challenge in recruiting participants [Rob11]. Even though the non-verbal cues the interviewer can get from the interviewee can be positive for the understanding, it also means that the interviewee can get non-verbal cues from the interviewer. People might be influenced by the dialogue with the interviewer and not tell their real opinions. This can also be a problem if the questions are biased [Rob11]. Another possible disadvantage with the interviews is that it can be hard to conduct the interview without previous experience. To ask follow-up questions directly and continuously analyze what the informant is saying during the interviews require training. Since the interviewer does not have any previous experience with the interview setting a test interview was performed. By performing a test interview, this disadvantage of lack of training decreases.

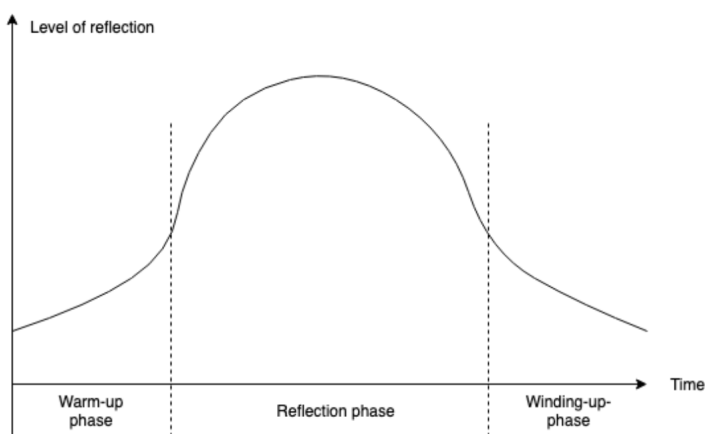
### 3.6.1 Recruitment of interview objects

Because this is a case study, the interview objects are recruited from the case organization. Interviewing the employees in the case organization gives information about the employee's experiences, which can give insight into the organization [Tjo10]. Information about the research project and a request to attend was posted to the organization's intranet. To get the necessary number of participants, we reposted the request two times. The change in email security solution that the organization is facing affects all employees in the organization, so there is no need to limit which employees can be interviewed.

Since there are 2000 employees in the case organization and only seven are interviewed, it is a small selection of the organization that is interviewed. This can be a problem because we will never know what information the rest of the employees have [Tjo10], and it can give a situation where vital information is missing, without us knowing. Therefore the analysis of the interviews focuses on what is common between several informants. There might also be that some groups are easier to recruit than others [Tjo10], which can be a problem when recruiting by open invitation. One example is that the people volunteering can be the employees that are most interested in information security, and thereby are more interested in this research project because they get to talk about a topic of interest for them [Tjo10]. Because of their interests, they might have more knowledge about the topics, and their answers might not represent an average employee. This is dealt with by evaluating their interest in the field during the interviews and in the recruitment process specifying that we are interested in all employees independent of their background.

### 3.6.2 Structure and content of the interviews

According to Tjora [Tjo10] an interview goes through three phases as presented in figure 3.5. Robson [Rob11] also supports this structure. He suggests introduction, warm-up, main body, cool-off and closure as the phases, where introduction and warm-up are equivalent to Tjora’s warm-up phase, the main body is equivalent to reflection phase and cool-off and closure are equivalent to winding-up phase. Different levels of reflection are expected in the different phases, and the questions asked are adapted to this expectation.



**Figure 3.5:** Tjora’s suggestion to the structure of an interview [Tjo10].

An interview guide that follows this structure is used in this research project and can be found in appendix C. The interview’s main body is divided into different sections, each covering one of the topics *security awareness and risk perception*, *user experience* and *trust and privacy*. Also, there is a section of the main body where the users are presented to emails that have been reported by employees in the case organization and asked to analyze the email. This analysis is included to compare what they do in the analysis with what they are answering to the other questions. It is also to see if there is any difference in their analysis of emails from before and after the new presentation of links and attachments. The questions in the interview guide were tested in the test interview to be able to adjust the questions in advance of the interviews if something were unclear. In addition, the interview guide was adjusted after the first interview. One question about suggestions for improving the user experience was added and one of the emails in the analysis part was replaced with two new ones.

### 3.6.3 The conduction of the interviews

Each interview took approximately 45 minutes, enough to get through all phases and ask the important questions. Tjora [Tjo10] recommends one hour or more for in-depth interviews, but because of time limitations and making the interviews easier to attend, 45 minutes were chosen as the time frame. Robson [Rob11] supports this and suggests that an interview should be between 30 minutes and one hour, because less than 30 minutes are unlikely to be valuable, and more than an hour takes too much time for busy interviewees.

It is important to create an interview setting that is comfortable for the interviewee and at the same time facilitates that the researcher gets to ask the planned questions [Tjo10]. The interviews were originally planned to be performed at the employees' workplace, but because of restrictions after the outbreak of the COVID-19 pandemic in Norway March 2020, they were all performed digitally. Both audio and video were utilized, as well as screen sharing to show email examples. The system used for this was Microsoft Teams<sup>5</sup>, which also has functionality for recording. The recording was used to ensure that nothing important is forgotten, and to be able to concentrate on the interview and ensure high-quality communication with follow-up questions [Tjo10]. During the interview only short notes are taken by hand, and right after the interview, a reflection note was written with the most important impressions. The interviews were also partly transcribed, meaning that everything the interviewee said related to the research was transcribed.

Due to restrictions because of the COVID-19 pandemic, there was no choice whether to perform the interviews digitally or face-to-face, but both has its benefits and disadvantages. Face-to-face interviews are preferred over telephone interviews when social cues are essential information sources [Rob11]. Another difficulty with a digital interview is that there is not a natural social setting, which can lead to a shorter interview because there is less small-talk [Tjo10]. The use of video and not only telephone decreases these problems because by seeing each other it is still a social setting and it is possible to pick up some social cues. Another difficulty with digital interviews is the possibility of technical issues, but the probability of this is decreased because the informants are used to the conference service. The technical issues can also be a natural starting point for small talk when checking that voice, audio and video are working. During the conducted interviews, there was no technical trouble. There are also some benefits to remote video interviews. Informants can feel less stressed with the physical absence of the interviewer and equipment because it feels less formal [Wel17].

---

<sup>5</sup><https://products.office.com/nb-no/microsoft-teams/group-chat-software>

## 3.7 Data analysis

To be able to interpret the collected data to answer the research question, analysis is necessary. The collected data is in different formats with various information and therefore requires different methods for analysis. The next subsections present the chosen methods.

### 3.7.1 Qualitative analysis of interview data

For analyzing qualitative data, Tjora [Tjo10] suggests a stepwise-deductive inductive approach. This includes going from data to theory and then going backward from the theoretic to the empiric. These two processes consist of several steps: *generation of empiric data, processing of raw data, coding, categorizing, development of concepts, discussion of concepts and creation of theory*. In our analysis, parts of this approach are used, but because of time limitations, we mainly focus on the inductive steps, going from data to a concept or theory.

A thematic coding approach is used to analyze the interview data, which is a qualitative analysis method. It consists in giving similar data the same code or label and group these codes under themes related to the research questions [Rob11]. Coding and categorizing are also two of the steps in the stepwise-deductive induction approach. The process is a constant comparison analysis, where the first data collected are assigned codes and then the same codes are used for the remaining data. The codes can also evolve through the analysis as more knowledge and insight are gained [Rob11]. The themes and codes used in this research project are shown in figure 3.6. The themes and codes are directly relevant to the research question, and the answers from the analysis of emails are mostly kept separate for a better comparison of the answers.

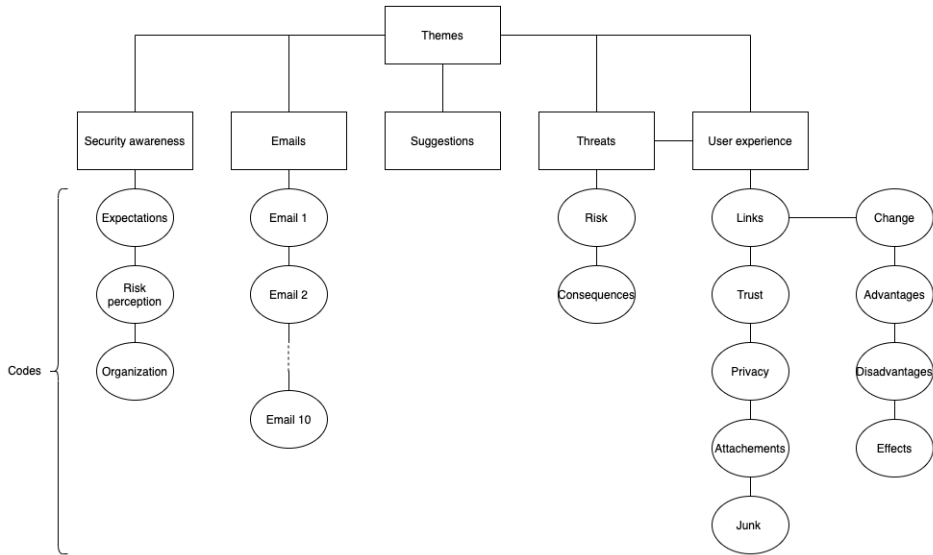
To organize and structure the transcriptions from the interviews, we used a program called Nvivo<sup>6</sup>. It is a program for analyzing quantitative data [Int20]. All transcripts were imported to this program, and the themes and codes in figure 3.6 were created as nodes. It gave an excellent foundation for comparing and analyzing the answers from the interviewees by getting different answers to the same topic side by side.

### 3.7.2 Analysis of reported emails

All the reported emails are in one inbox with emails dated from 2016 and up till now. A structured analysis where all emails are checked and counted, probably through the use of a script, would be ideal, but due to time limitations and limited gain for our

---

<sup>6</sup><https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home>



**Figure 3.6:** Overview of themes and codes used in the analysis of the interviews.

research objective, it is not done. Instead, the focus is on the content of the reported emails. The analysis performed consisted of looking through the inbox and reading many emails. The work consisted of finding patterns between the emails, for example, by seeing that many employees reported the same email. Another important part of the analysis was to see if there are any significant differences in the emails reported now and from before the new email solution was implemented. When doing this, we specifically investigated if there are now more emails with links that are reported.

Some of the reported emails were used during the interviews, and they were carefully selected. It is crucial to have a varied selection to get to know all possible evaluation criteria the employees might have. It is also essential that there are emails from before and after the implementation of the new solution, to be able to analyze if there are any differences.

### 3.7.3 Analysis of conversations with the security manager

The analysis of the conversations with the security manager in the case organization, consist mostly of understanding what has been said about their systems. This is done by seeking more information online. In addition, it has been essential to structure the information to be understandable for the reader. Later, to see this information

in the context of the interview results are an important part of the complete analysis for discussion.

During the conversation, the security manager provided some numbers on responses to phishing emails. It can be looked at as qualitative data turned into numbers, and it does not require advanced statistical analysis [Rob11]. Therefore the numbers are presented graphically, and these graphs are made using Google Sheets<sup>7</sup>. The analysis is a frequency analysis, where the number of times an event happens is counted [Rob11]. In this case, these events are how many clicks a link in the received phishing email or how many report the email as suspicious. A bar chart presents this data with the vertical axis representing the quantity and the horizontal axis representing the different events.

### 3.8 Case context

This research project carries out as a case study. Case study as a research method investigates a contemporary phenomenon in-depth and in its real-life context. It helps to answer research questions asking *how or why* [Yin09]. Since this project's objective is to look into a current change and how this affects security culture, a case study is appropriate. Yin [Yin09] suggests four types of case study designs, and for this research project a *holistic single-case* design is chosen. It means that it is one case that is investigated and that the global nature of the case is investigated instead of having an interest in special subunits [Yin09]. One organization is chosen as the case and is referred to as the case organization. The organization is chosen because it is now undergoing the relevant technological change that this research project investigates. The underlying technology of their implemented systems is the focus, not the specific systems. This focus is selected to make the results more general, as it is this case organization that is the source for data collection.

The case organization is a knowledge organization with 2000 employees, and they focus a lot on security awareness among the employees. In the organization there are people with many different professions, and there is also administrative staff with a different background. All these employees, therefore, have a very different basis for risk perception and understanding of their responsibility for the organization's security. The organization has an ongoing security awareness campaign to train its employees, which has been ongoing since 2014 to different extents. The campaign includes short videos, e-learning sessions, surveys, phishing emails and general information and reminders. The employees' possibility to report emails they find suspicious is also a part of this campaign.

---

<sup>7</sup><https://www.google.com/sheets/about/>

The IT department has sent constructed phishing emails to all the employees for education and increasing security awareness, and all with different focus. The first was to check if the employees used mouse-over to reveal a different link, and 885 employees were registered to click the link in the email or the attachment. In 2015 the phishing email was constructed to check if the employees would provide their password to a password control, and 23 of the employees did so. Only one of them notified the IT manager afterward. In 2016 they implemented the function for reporting emails, so the phishing email was sent out to check how many reported it, and 560 did report it.

Regarding the security systems in the case organization, they started using a SIEM platform in 2019. The platform was chosen because it gives a comprehensive presentation of the security situation in the organization. The SIEM solution uses information from many different sources, including all employees, devices, programs and the infrastructure. It contains an ATP, which further includes the email protection and analyze all incoming emails. The analysis performed is based on machine learning and big data. There is big amounts of data from within the organization, but the SIEM system also facilitates the use of data from many other organizations in the analysis. With advanced algorithms, it is, therefore, possible to notify security breaches in many different forms, including zero-day attacks.

### **3.9 Ethical considerations and privacy concerns**

For this study, necessary ethical consideration are the privacy of the informants and the confidentiality of the research data. The privacy of the informants is a concern because we gather personal information, both email address and name, and do audio recording of the interviews. Therefore the research project was reported to the Norwegian Centre of Research Data<sup>8</sup> before the data collection started, and the approval can be found in appendix D.

Regarding the interviews, precautionary measures were taken to ensure the privacy and confidentiality of the interviewees. Before the interviews, an information sheet was provided to all the participants with information about the project and their rights. The information sheet is in appendix A. To ensure all necessary information was provided, a template created by the Norwegian Centre of Research Data was used. The interview objects also had to give their consent before the interview. After the interview, the audio records were securely stored encrypted with access control to ensure the confidentiality of the data. To decrease the ethical issues, all the participants are anonymous in this report, which is considered normal practice [Rob11].

---

<sup>8</sup><https://nsd.no/>

For the use of information from the reported emails, the employees in the case organization that has reported emails were informed about the use of the emails for this research through the information sheet in appendix B. They were also informed about their rights and had the opportunity to omit their emails from the research. The employees are not recognizable in this research report.



# Chapter 4

## Results

This chapter presents the data that is collected with the methods presented in chapter 3. First, the outcome from the conversations with the security manager in the case organization is presented in section 4.1. Then, findings in the inbox with reported emails in section 4.2 and lastly the results from the interviews in section 4.3. Further these results are discussed in chapter 5.

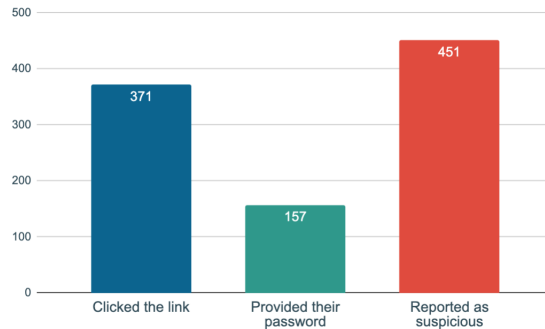
### **4.1 Information from conversations with the security manager in the case organization**

The conversations with the security manager in the case organization gave insight into the organization's security culture and their choices regarding security solutions. The talks also provided information about their security awareness campaigns. This section presents information from the conversations.

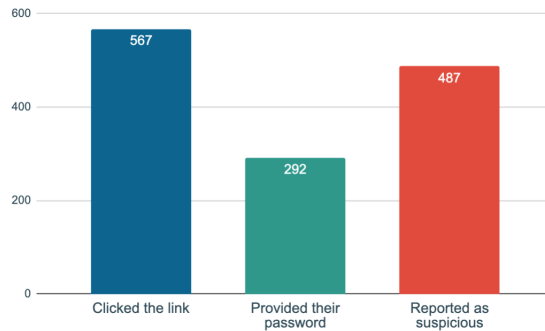
#### **4.1.1 Results from a phishing campaign**

The security manager provided results from the previous phishing email they sent out, which was fall 2019. That was right before the implementation of the new email security solution. The phishing campaigns are a part of the ongoing security campaign in the case organization, where they send constructed phishing emails to all their employees to see how they act on it and for the employees to learn typical examples of phishing. The phishing email was carefully constructed to imitate a real phishing attempt and was apparently sent from the human resources department. As described in the pre-project report [Sel19], the email was first written in English and translated with Google Translate to Norwegian. All emails included the name of the receiver to make it personal. The email said that the organization now is implementing a new salary system and that every employee has to click a link where you can log in and check if the salary is registered correctly. To log in, you have to provide a username and password [Sel19].

Every employee in the case organization received the email, and figure 4.1 and figure 4.2 shows the results. The pre-project report also presents these data as preliminary results. 24 hours after the email was sent out, out of the 2000 employees, 18.4% had clicked the link and 7.7% had given away their password. The results indicate that these people did not perceive the email as suspicious. Also, there were 22.4% that used the functionality to report emails and reported this email during the 24 first hours. The results after seven days show that 28.1% have clicked the link at this time. Because of many reactions from the employees, they revealed that the email was a part of the campaign a short time after it was sent. The results after seven days might be affected by this in the way that people click the link just to see what happens [Sel19].



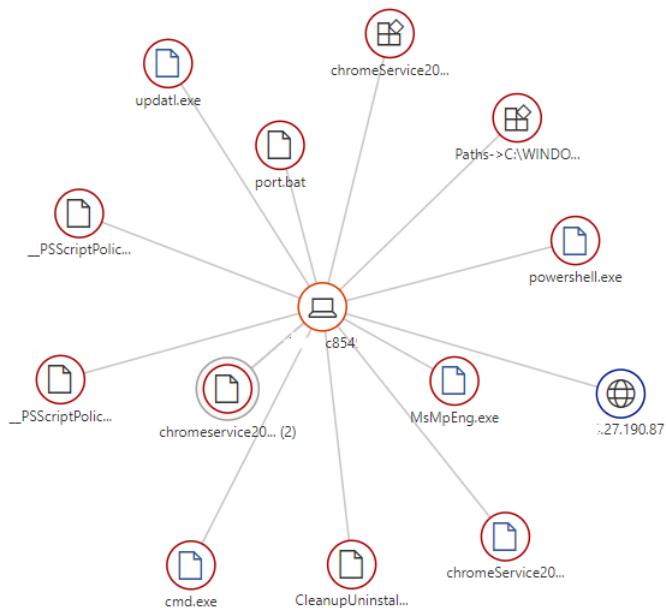
**Figure 4.1:** Results 24 hours after phishing email was sent fall 2019. The vertical axis representing the number of employees out of 2000. Figure from pre-project report [Sel19].



**Figure 4.2:** Results seven days after phishing email was sent fall 2019. The vertical axis representing the number of employees out of 2000. Figure from pre-project report [Sel19].

### 4.1.2 The new security solution

The main reason for implementing the new system is to increase security by handling security breaches faster, and therefore the organization chose to implement a SIEM solution. The SIEM platform makes it possible for the administrators in the organization to find the context around a security breach in a much shorter time. If the administrator gets an alarm regarding a computer in the organization, the administrator can easier check the corresponding alerts and find the reason. It is also attached a severity degree to the alert. One example is that a user can have downloaded malware on their computer that fetches passwords and sends them to the attacker. When the system notifies the administrator about the incident, they can open a graph in the SIEM platform, like the one in figure 4.3. The graph shows what has happened on the computer that can be related to the attack, for example, that it has contacted an IP address on the web, ran a power shell and deactivated the antivirus. The administrator can also see where the malware came from, for example, whether it is through clicking something in the web browser or through an attachment in an email. If the attacker has used the password to get access to some services, the system can also reveal that.

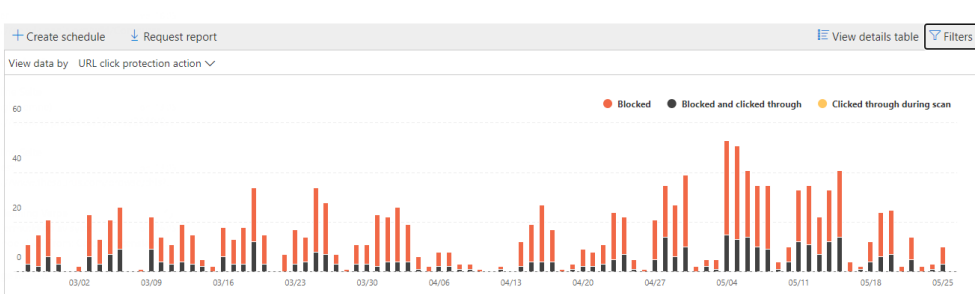


**Figure 4.3:** Example of the graph presentation of an incident in the SIEM solution implemented in the case organization. Each node can be clicked for more information about the specific action.

That kind of advanced analysis is possible because now all systems in the organization are connected to the SIEM. Earlier, they had one system for network errors and firewalls, one for antivirus and one for surveillance of the active directory, and they all created separate reports. If one of the reports included an incident, the administrator had to manually find matching events in the other reports. For example, if the antivirus reports an incident, the administrator has to check in the active directory report if the user has logged in and in the network log to see what the user has visited.

For email specifically, there is an improved functionality to identify an email containing malware and what damage this email potentially can do. To be able to perform this analysis, the SIEM gets data from several sources, including the email server, sandbox testing of links and from the antivirus. The increased amount of data and improved algorithms enable better filtering, with the goal of smaller amounts of undesired email in the user’s inbox. Since this system is based on machine learning algorithms, the system will increase the performance over time. The system works in the way that a link is analyzed in a sandbox when the user clicks the link if the email is not already identified as malicious by the system. Since an attacker can change what is behind an URL after the receiver has received an email, it would not be enough to check the email before it reaches the user’s inbox. If some malicious code is detected in an email during analysis, the email is removed from other users’ inboxes if they have received the same email.

To further understand the effects of the solution on email security, the security manager presented the graph shown in figure 4.4. It is an example of both what kind of information the system administrator is now able to get and it also shows the performance of the system. The graph also says something about how threatened the case organization is by providing a summary and trend view for detected threats and actions taken on URL clicks.



**Figure 4.4:** Graph from the case organization’s SIEM solution showing statistics on blocked URLs between February and May 2020.

Even though the change is significant for the administrator, the change is not that evident for the user, except for in the email solution. Many of the systems are the same even though they are connected, and therefore there is no change for the user who experiences the systems separately. One thing they see is the change in the email security solution, where the presentation of links is different. The complex analysis leads to a new presentation of links and attachments to the user. Most links get a new prefix, and figure 4.5 shows one example of a link with the new presentation. The security manager says that they do not want to use the new presentation of links on internal emails, but they have tried to turn it off and it has been some problems with the adjustments. Further, he says that there was some fuzz around the new presentation in the very beginning, but people are getting used to it.



**Figure 4.5:** Example of the change in presentation of URLs with the new email security solution in the case organization.

Because of the high degree of automation with the SIEM solution, there is also a possibility for false positives, which has to be handled. The algorithms used will not always be correct, especially in rare types of cases. The solution to this now is to add extra surveillance on a computer if there is any uncertainty about whether or not it is infected. Soon the organization is planning to include a new alarm system for the user directly in the SIEM solution. The new system includes that the user automatically gets alarmed about their actions if something suspicious is detected, so that the administrator does not have to inform the user manually. When the user receives an alarm, they can quickly notify whether a benign action triggered the alarm or if it is unexpected and may be malicious. This means that if it is a false alarm, the user can easily notify the system instead of the administrator having to lock down their computer. One example is in the case where an alarm is triggered if a user logs in to a system from England right after being located in Norway. The new system notifies the user about this, and if the user logged in from England because of using a Virtual Private Network (VPN) connection, they can notify back that this

is just a false alarm. With this mechanism, the system is gradually learning, and by that becoming continuously better and decreases the number of false positives.

## 4.2 Findings in the reported emails

The first observation when briefly overlooking the inbox with reported emails is that there is big amounts of spam. Many employees report the same emails, and figure 4.6 shows an example of such an email. This email, and most of the other reported spam emails, are also attempts at phishing. The email in figure 4.7 is an attempt at phishing and is also a typically reported email.

When looking through the inbox with reported emails, there is hard to see any significant differences. There is no difference in the type of emails reported before and after the implementation of new security systems on email, and there is neither any notable change in the number of reported emails. The security manager says that he neither has notified any significant differences in the reported emails. Further, he says that other factors can lead to more recognizable changes. For example, after an intense campaign period, the number of reported emails increases.



**Figure 4.6:** Example of spam email from the inbox with reported emails.

## 4.3 Interview findings

The following section presents the results from the seven interviews under different topics. The two first topics are security awareness and user experience, which correspond to the interview's main body and directly connect to the research question. Then there is one section with suggestions for improvement, and lastly, the results from the part of the interview where the interviewees analyzed reported emails are presented. In the text, citations from the interviews are used to highlight essential points. Because it is a semi-structured interview, not all the questions were asked every participant in the exact same way, the focus was to cover all the topics.

## PURRING

DF Desmond Frempong <Desmond.Frempong@stami.no>  
 Hi, 21.04.2020 12:57  
 Til: [REDACTED]  
 Kopi: okonomi <okonomi@stami.no>

Hei,

Ved gjennomgang av Deres konto hos oss kan vi fremdeles ikke se at fakturaen ble betalt (Se kontoutdrag nede). Kan de betale beløpet til Statens Arbeidsmiljøinstitutt sin bankkonto: 7694 05 02027 og merke med fakturanummer.

Dersom denne faktura ikke blir betalt innen 14 dager fra dags dato, vil krevet bli sendt til inkasso.

Analysér Oppsett Val Statistikk Besøksloggen Utligget Innbetalte sjøker Vis arbeidsdyktart

Ny kobling Organiser koblinger

Kunde: [REDACTED] FIDE

Sjøløst: SINTEF. Cx Fakturamottak Postboks 4515,0208 NO-1100AA

N	Kunder	Fakturanr	Fakt.dato	Forfall	BA	R	S	Konto	Val	Valutabeløp	Best valuta	Per	Bilaggr	Tekst	Beløp
1	C	4826	71900427	31.12.2019	30.01.2020	FA	N	1500	NOK	50 000,00	50 000,00	201912	71900427	ROL 19/00256 SINTEF 122019	50 000,00
2	C	4826	71600173	10.05.2016	09.06.2016	FA	N	1500	NOK	539 000,00	0,00	201605	71600173		539 000,00
3	C	4826	000000000	10.06.2016		OC	N	1500	NOK	-539 000,00	0,00	201606	81660069	1048260716001733	-539 000,00
4	C	4826	71600332	05.12.2016	05.01.2017	FA	N	1500	NOK	539 000,00	0,00	201612	71600332	DL201400426 SINTEF 122016	539 000,00
5	C	4826	000000000	06.01.2017		OC	N	1500	NOK	-539 000,00	0,00	201701	81700003	1048260716003329	-539 000,00
6	C	4826	71700080	06.02.2017	08.03.2017	FA	N	1500	NOK	3 800,00	0,00	201702	71700080	Eine Blom Hoem	3 800,00
7	C	4826	135601050	08.03.2017		OC	N	1500	NOK	-3 800,00	0,00	201703	81700029	1048260717000803	-3 800,00
8	C	4826	71700281	30.08.2017	09.09.2017	FA	N	1500	NOK	539 000,00	0,00	201708	71700281	DL201400426 SINTEF 082017	539 000,00
9	C	4826	000000000	11.09.2017		OC	N	1500	NOK	-539 000,00	0,00	201709	81700098	1048260717002814	-539 000,00
10	C	4826	71700343	02.10.2017	01.11.2017	FA	N	1500	NOK	575 000,00	0,00	201710	71700343	201400426 SINTEF 102017	575 000,00
11	C	4826	000000000	01.11.2017		OC	N	1500	NOK	-575 000,00	0,00	201711	81700119	1048260717003438	-575 000,00
T										50 000,00	50 000,00				50 000,00

Med Vennlig hilsen/ Best regards

**Desmond Teddy Frempong**

Department of Administration

Statens arbeidsmiljøinstitutt (STAMI)/ National Inst. of Occupational Health

Direkte/Mobil: +47 23 19 51 33/ +47 95 41 95 20

Sentrallbord: +47 23 19 51 00

Fax nr.: 23 19 5201/00

[www.stami.no](http://www.stami.no)

Besøksadresse: Gydas vei 8, Majorstua, Oslo

Postadresse: Pb 8149 Dep, 0033 Oslo



Figure 4.7: Example of phishing email from the inbox with reported emails.

### 4.3.1 Security awareness

To get insight into the security awareness of the employees, a focus during the interviews was how they perceive the threats against their organization and what they do to avoid these.

**Perception of the threats against the case organization** When asked about which threats their organization is exposed to through the use of email, all seven interviewees provided answers that indicate good insight. They all focused on the threats of attacks targeted against their organization. However, one interviewee also mentioned the possibility of being a victim of more random attacks sent to a bunch of different email addresses:

*"It is two-sided: one is the ones that send emails to all email addresses they find, and we are exposed to this because our websites provide names and emails of all employees. Nevertheless, it is worse with the targeted attacks, they who try to get access to our organization specifically."*

Further, there were observed two different perspectives on the threats among the interview candidates. Two interviewees talked about the threat where people with malicious intentions capture information sent in emails. The other five of the interviewees talked about the threats coming from an outsider that gets access to their systems and intranet. This access can give rights to open files and retrieve secret documents.

Regarding how an attacker can introduce a threat to the organization, different suggestions were proposed. Five of the interviewees mentioned the threat of malware, and specifically the threat of ransomware. Two interview objects specifically mentioned the incident that happened when Hydro was exposed to ransomware, as an example of something that also is a possible threat to their organization. Direct economic fraud is also mentioned as a threat, for example, someone pretending to be their boss and asking them to pay an invoice.

All interview candidates gave answers that indicate that they understand that information they have in their organization is secret and that it has severe consequences if the information is stolen or blocked. Consequences mentioned in the case of an attack where someone has stolen information are monetary loss and loss of reputation. One interviewee says this about the consequences of loss of reputation:

*"If someone steals business-critical information about some of our clients, it will lead to an awfully bad reputation, and reputation is very important for a knowledge organization"*

A more directly personal consequence is identity theft, and one of the interviewees mentioned that as a possible consequence if an attacker gets insight into personal information the organization has stored about an employee. One of the interviewees also underlines that the consequences in all cases depend on who gets hold of the information.

Some of the participants were asked how they affect the security of the organization through the use of email. One of the participants answered:

*"Every time I click something or opening something in an email I am participating in exposing us to risk. So the security in our infrastructure is not more secure than the 2000 of us that is opening things in email, so we are all responsible."*

Two of the other participants also answered that they are an important part of the filter for malicious activity. Through the conversations during the interview all



participants showed understanding of their responsibility.

**How the employees avoid threats** When asked how to avoid the identified threats, they mainly answer what they look for in an email to reveal malicious intentions. All interviewees are aware that clicking links and opening attachments can cause danger. Most routines involve checking the context and content of the email and based on that decide if the link or attachment is safe. Also, five of the interviewees gave answers that indicate that the syntax of the URL and the name of the attachment matter.

All of the interviewees said that to decide if the received email is malicious, the first thing they do is to determine if they expect to receive the email. Regarding this, two of the interviewees identified the threat of someone pretending to be a partner, and one of them said the following:

*"If it is a partner that I have a dialogue with, I don't check anything more, but when we are talking about this now, I realize that there is a risk if someone copies a legal email, then they can fool me."*

Another problem with using the expectation as a filter is that the organization receives many emails from unknown people. One interviewee describes a dilemma regarding this in the following way:

*"In our organization, the majority are sellers, so we have to be open to suggestions and questions from unknown people. The balance between being attractive and curious about new things, and at the same time being restrictive with everything unknown is difficult."*

When an email is not expected or they find that something is suspicious, they all have routines to investigate whether the email is malicious. The most used method is to check the sender's email address. Three of the respondents say that they compare the sender's name with the actual sender's address by holding the pointer over the name. When the interview candidates are asked to evaluate a set of emails later in the interview, all of them are performing this method for evaluation. A deviation between the name and address leads to skepticism, especially if the email domain is unexpected. If they are still uncertain about the email, there are different procedures among the interviewees. One of the employees mentioned the language as an essential factor for the analysis of an email. Three of the other respondents say that they check the email headers to see which servers the email has passed. There they look for reasonable domain names on the servers. One also checks if they have signatures on the servers because the emails in the organization are seldom encrypted or signed

end-to-end in the organization. Another employee has, on some occasions, forwarded the email to a private phone and opened the link there if they are unsure about the intentions behind the email. Further, two others mentioned that it is suspicious when they receive an email with only a link or an attachment, and no text. Another method to handle the threats is to read the email in plain text format, and one of the interviewees says this:

*"I always turn on plain text if the system allows it. ... Plain text usually does not do any damage unless you actively do something."*

A general strategy among the interviewees is that they seek more information if they are uncertain whether to click a link. Two employees say that they search for the sender or company on the Internet to see if the firm is real and get others' experiences. Another two of the interviewees say that if they are unsure about a link, they open it by writing the search path in a browser instead of clicking the link. One of the respondents says that one solution is to ask the IT department when unsure about an email. This person, along with two other respondents, says that if they are still unsure if the link or attachment is safe to open, they call or email the sender and ask if what they have received is legitimate.

To open received emails on a computer instead of a phone is also a tactic they use. Two of the interviewees say that they think it is easier to evaluate the links on their computer than on their phone, and one of them always opens emails on a computer. They can see the full link more efficiently on a computer, and they can use mouse-over to see the actual link on HTML hyperlinks. One of them also specifies that it is easier to see the design of the email on the computer than on the phone because of the small screen.

One of the interviewees that focused on the threat of sending confidential information over email uploads the document to a shared folder and send the link to this folder on email, instead of sending the information as an attachment. This procedure makes it harder for a potential attacker to get hold of the information.

If they find an email to be suspicious, five of the interviewees say that they report it with the organization's function for reporting malicious emails. The other two delete it, and one of them says it is because of laziness that they are deleted instead of reported.

**What they think the case organization does for email security** In the first part of the interview the participants were asked what they think their organization is doing to handle malicious email. All interviewees answer that they assume that the organization is doing some kind of filtering, including that a lot of spam is filtered out

before it reaches the user. To the same question, three of the interviewees mentioned that the organization has implemented a function for reporting suspicious emails directly from the inbox. Two of the participants also mention that they have ongoing campaigns to increase knowledge and security awareness. Further, another two of the interview candidates answered to this question that the organization recently introduced analysis of links, and about this one of them said:

*"I know that recently the links have gotten extra code, I don't know the technical details behind it, but I guess that it is making us more secure. That is the most important."*

### 4.3.2 User experience

As a big part of this research project is to investigate the user experience of the new parts of the email solution, the interview had a considerable focus on how the users are affected by these new functions.

**Detection of changes** The first question on user experience asked if they had recognized any changes in the email system during the last six months. From this question, we wanted to know if the interview candidate had recognized that it was now implemented analysis of links leading to a more extended and more unclear presentation. Before this question was asked, five participants had already mentioned this new function. One of the participants cannot remember any changes, but when asked specifically about changes in links, the answer is:

*"I have not thought about it, but I can remember that we were told that there was added some security to the links. One time I had to copy a link instead of clicking it, but that only happened once."*

Further, when asked specifically about the new implementation of links, the person remembers. The other person that had not mentioned the new presentation of links immediately answered the analysis of links as a new function in the email solution when asked this question.

**Analysis of the new links** An important result is that out of the seven asked participants, four thinks that the rewritten links are harder to interpret than the original, one thinks it is easier and two think that there is no difference. When asked about if it is harder to know the original URL with the new presentation, the one that thinks it is easier now says:

*"The new function makes it much easier. It destroys the URL, and then you can see much easier if the domain name is correct. ... The link is*

*longer, but in return it is more often visible, so you can see the domain name if you just know where to look."*

One of the interviewees that think it is the same says:

*"No, that is not a problem. I look in the long link, I have no problem with finding the relevant information there, it takes a second or two longer, but it doesn't matter to me. "*

One of the other participants that think it is more challenging to analyze the links by yourself now says:

*"Instead of seeing where the link actually leads to, I have just the long and complex link. I have just given up on interpreting the link because it is very long and hard to see,..."*

**Advantages with the changes** There were mentioned several advantages with the visible changes during the interviews. The advantages that the interviewees mentioned are that someone has filtered out the worst cases before emails reach the user's inbox, fewer responsibilities to the users and easier to use. Another advantage is the consistency of a technical tool compared to human decisions, and one of the interviewees says this:

*"To some extent it can make me less conscious, but I think it is a reasonable technical tool that weighs out the disadvantages. I guess it is more consistent than I am. If a phishing email hits at the right time when I am expecting something, then it is probably less vulnerable than I am."*

One of the interviewees are very neutral to the new presentation of links and says:

*"I think that it is positive if it is able to catch something, and there are no disadvantages for me. So for me there is no difference, but I think the organization in total is better equipped."*

**Disadvantages with the changes** During the interviews, there were also mentioned several disadvantages with the new presentation of links. From the previous interview quote, a disadvantage is that the user can become less conscious. This limitation was mentioned as a consequence of increased trust in the analyzed links. Another disadvantage that was mentioned is that it is harder to do the evaluation

of received links yourself and that the solution, therefore, can make the user's less aware.

There were also some limitations directly to the functioning. One of the interviewees mentioned a problem a colleague had with a registration link to a website that did not work after being extended after analysis. Another problem mentioned is the reusing of links and, thereby, forwarding emails with links that have already been rewritten. One of the interviewees also found it more complicated to read the extended link on the phone than the original link.

**Satisfaction with filtering of junk and spam** The participants were asked how they experience the system's ability to determine which emails are spam and should be forwarded to the junk folder. All of the interviewees say that they are satisfied with this filtering, and no one had noticed any change in the filtering before and after the new security solution was implemented. The only thing that is mentioned about the development of the filtering is that one of them says that it continuously becomes rarer with spam in the main inbox. About the filtering, one of the other interviewees say:

*"It works well for me, but I hear people complaining about it. Of course, there is something that ends up in the wrong place, but that is a part of having protection, it cannot always be correct."*

Another one specifies that there is not much in the junk folder that should have been in the main inbox:

*"I sometimes check the junk folder, but it is not much there, maybe some advertising. It is not many times that I have had to fetch emails from the junk folder."*

**The participants' trust in the solution** One of the questions in the interview was about whether the interviewees trust the security solution. The answers to this can be partitioned into whether the interviewee expresses trust in the technology or the IT department in the organization. In general, all of the interviewed employees say that they have trust in the system, except for one. The one that does not trust the system say:

*"No, I have no reason for that. Trust is something that grows, and for me, it is based on experiences."*

Two of the interviewees say they trust that the IT department makes the correct decisions about the security systems used in their organization. One of them says:

*"When our experts have decided that we are going to use a system and introduce it, I trust that system and assume that they have taken the right decision."*

One of the participants specifies the following:

*"It doesn't mean that I can click everything and don't do anything myself. It is a supplement, but I still have to do things myself. I trust that what they filter out are things I am not missing. Because of this, I more rarely analyze the email because I get less spam, but I still have to be aware."*

This is a contrast to two of the other interviewees that trust the system and the links in a way that fully trusts the analyzed links. One of them say:

*"Now they have started to scan the links in advance, and that is good, but I can't check the links myself, so I just have to trust that the scanning works."*

Six of the participants were also asked if they expect that such solutions are always correct and can be fully trusted. Three of them said they expect that, and the other three said they do not expect to trust the system entirely. Reasons that are mentioned for not expecting the system always to be secure are that there are constantly new ways to trick people that the system does not know about, and there can be bugs in the system. One of the participants expects the system to catch spam, but not malicious emails targeted directly against a person.

**The participants' perception of privacy protection** Towards the end of the interview, all the participants were asked if they feel that their privacy is protected through the use of the email system and the security solutions. The general answer is that the participants are okay with the system having access to their email. Six of the participants say that it is okay, and the last one feels like there is no other choice than to accept it. Two employees justify this by saying that you should not demand privacy on your work email. One of them, among two others of the asked, also says that it is okay because they feel like they have nothing in their email they have to hide.

The interviewees were also asked if they know how the system can do the necessary analysis, and three of them answer that the system needs insight into the email to do the necessary analysis. One of them says:

*"I am fully aware that they look at the content, and I think that is completely okay, I don't worry about it. The benefits weigh more than if I were to think that it is unpleasant."*

**Effects on security awareness** During the interviews some of the participants directly mentioned their security awareness, even though they were not directly asked about it. When asked about the pros and cons of the new system, one of the interviewees first said this:

*"The new presentation of links shows me that there is a system that helps to watch out, but whether it makes me more aware or relaxed, I am not sure if I know the answer to."*

About security awareness, another interviewee says:

*"I can imagine that the new presentation and analysis of links have made the threshold low enough so that I will just click the link to see what it is. That is if it is not too abnormal, which would lead me to change mode, but I guess that it is before you slow down and check things carefully that they have the opportunity to make you click the link. And in that case, I am not sure if the new function helps unless they actually have checked the link."*

Another of the interviewees says this:

*"I always make an assessment and try to see if it seems plausible, and that is not always easy to recognize. Now we have a new system that rewrites the links, so now you can't see and evaluate the link. It is meant to shield us. At the same time, for me, as a user, I can not make an informed choice anymore, whether to click or not. If anyone can bypass the system, it is harder for me to determine. If there are emails that clearly are not for me, I will not follow the links. It is possible to trick me too, but then the content has to be something I am expecting or be specific for me to some degree."*

Two of the interviewees said directly that their evaluation of links was not affected by the new function. When asked if they assess emails any different now, one of them answered:

*"The analysis is an aid, but in the last instance, it is my evaluation that is the endpoint for whether I am opening something or not. If the link is analyzed or not doesn't matter."*

### 4.3.3 Suggestions for improvement

After the first interview, a new question was added to the interview guide to investigate if any of the participants had suggestions for improvements to the system. The idea for this question came because the first interviewee suggested improvements without being asked. Out of the seven interviewees, four of them had concrete suggestions for improvements or new functions. Two of the interviewees are satisfied with today's solutions and do not see the benefit of adding more functions. The last interviewee does not have suggestions on new functions in the email solution but wants more education on email security. The following was suggested during the interviews:

**Categorizing of email** Two of the interviewees suggested adding a visible categorizing of email, a technical function that can be implemented instead of trusting people to do the evaluation. One of them suggests a classification based on how suspicious the system finds the email, and think that would be useful because the user can change mode based on the system's classification of the email. It should not be too hard since they are already doing an analysis. According to the interviewee, the reason to include this function is that with the new analysis of links it is harder to do an evaluation of the email themselves:

*"I think that it is okay that they do the scanning, but for me, it is harder to make a decision since I can't see the original link."*

The other suggestion for classification is to base it on a confidentiality level. This function can, among other things, include that emails marked as internal cannot be sent to external receivers and if the email is marked as confidential it is not possible to add an attachment. According to the interviewee, the email solution they use in the organization already has support for adding a confidentiality level to emails.

**Warning on sender address** One of the interviewees suggested adding a warning sign if the sender is suspicious. This can be helpful when the user is in a hurry because fake email addresses can look like valid email addresses with only small changes, which can be hard to detect.



**Easier access to email header** During the interview, three of the participants mentioned that they use information in the email header to evaluate the credibility of an email. One of them suggested that this should be easier accessible, where the user can click one button to access the message header.

**Plain text emails** Two of the interviewees suggest to use a text-based email solution instead of HTML. This measure would, for example, make the URL appear in the email instead of overwritten text like "Click here". In addition, the links do not have to be clickable, but instead, copy and paste can be used to open the URL in a browser.

**Digital signature on emails** One suggestion is to use digital signatures to sign emails. It works in the way that the sender signs the email before sending it using a key or certificate from someone trusted, and then the receiver can check that the correct sender signed it. This means that the receiver, to a certain degree, can verify the sender. The interviewee means that this would be significant progress.

**More education** One of the interviewees wants more educational videos instead of more function to the system, and said this:

*"To get a reminder, short videos are a very good way to remind the employees. I think it should be done regularly, that you almost every month get a reminder about the videos. I quickly fall back into old habits."*

On the other hand, one of the other interviewees stresses the need for technical functions because you can never be sure what the users do despite more education:

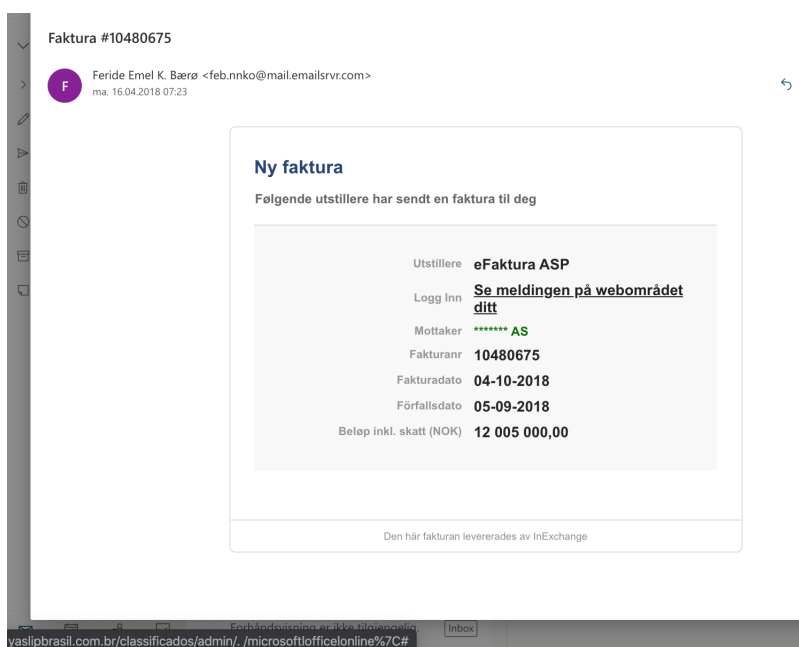
*"Up till now I have thought that it is impossible to make sure that employees don't do anything stupid when receiving an email and that you just have to make sure that the suspicious emails don't reach the user's inbox."*

#### 4.3.4 Analysis of reported emails

During the interviews, the participants were shown a set of emails and asked what they would do if they received the email in their inbox. Some of the emails were from before the implementation of the new security solution, and some from after. It was hard to get to know how the interviewee analyzed only the links. Instead, the exercise gave input to how the interviewee analyzes an email and how vital the link layout is for their consideration. It is also interesting to see when the consideration of links becomes necessary to evaluate an email.

For each email, the interviewee was asked how they evaluate the email and why. Here follow the responses to each email:

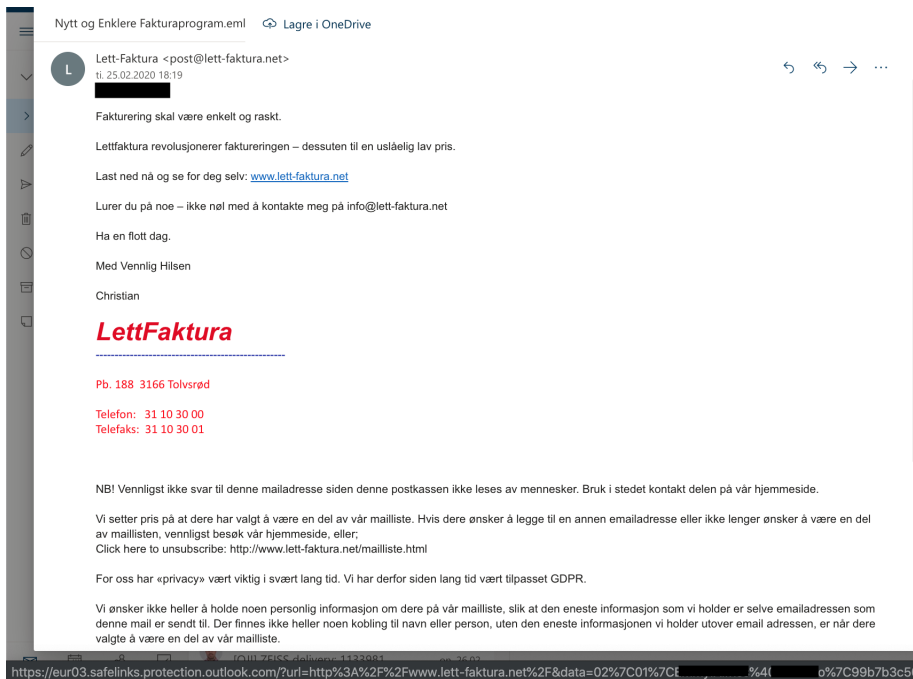
**Email 1 (figure 4.8)** The first email is a fake invoice, and all of the interviewees find this email suspicious. They all mention the sender's address as a sign that this is something malicious. Further, three of them say that they are not supposed to receive emails like this, and three of them also react to the enormous amount. By using mouse-over on the link saying "Se meldingen på webområdet ditt", the link in the bottom of the figure appears. One of the interviewees starts by mentioning that it is a strange URL with "yaslipbrasil.com", and says that the fact that it says "brasil" leads to skepticism. On the other hand, two of the participants specifically say that they would not even consider the link by using mouse over to see the URL, because other factors in the email lead to the email already being deleted or ignored. The remaining four participants are not mentioning the link as a factor in their evaluation of this email.



**Figure 4.8:** Email number 1 of the analysis of reported emails during the interviews. Received before implementation of the new security functions.

**Email 2 (figure 4.9)** This email is an advertisement for an invoice service, and six out of the seven asked participants say that this is just marketing and that they are not in the target group. They do not think it is suspicious, but two of them say they would have done some research on the company if it was relevant. The last

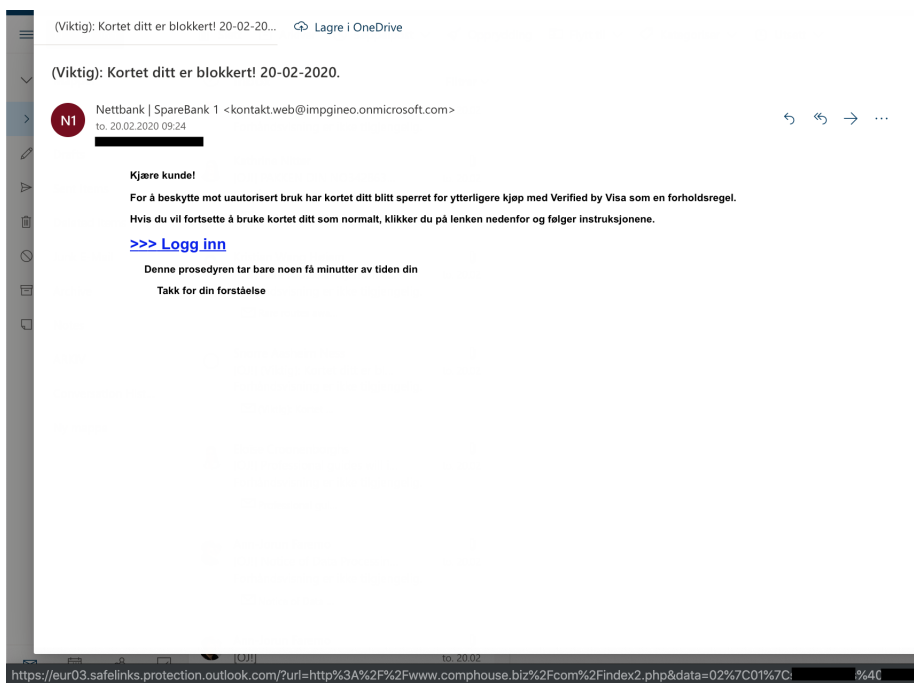
person says that it is a bad language and that the email would have been deleted.



**Figure 4.9:** Email number 2 of the analysis of reported emails during the interviews. Received after implementation of the new security functions.

**Email 3 (figure 4.10)** The third email is from a bank asking the receiver to log in through a link to open a blocked credit card. The URL behind the link saying "Logg inn" is shown using mouse-over, and is an analyzed link. Six of the participants say that the email is not real because a bank would never ask you to log in through a link in an email. Four of them also mentioned that the sender's address is strange. On the other hand, there is one of the interviewees that think that the sender's address could be real, but understand that the email is malicious because of the content. One of the interviewees says this:

*"I never log into banks through emails. I would have deleted this because of that, but if I were to evaluate it, I would have seen that the link is weird. ... I can see that it says "comphouse" in the link, I am not sure if that is were you are directed, I feel that I am being tricked because it says that the link is checked through the analysis."*



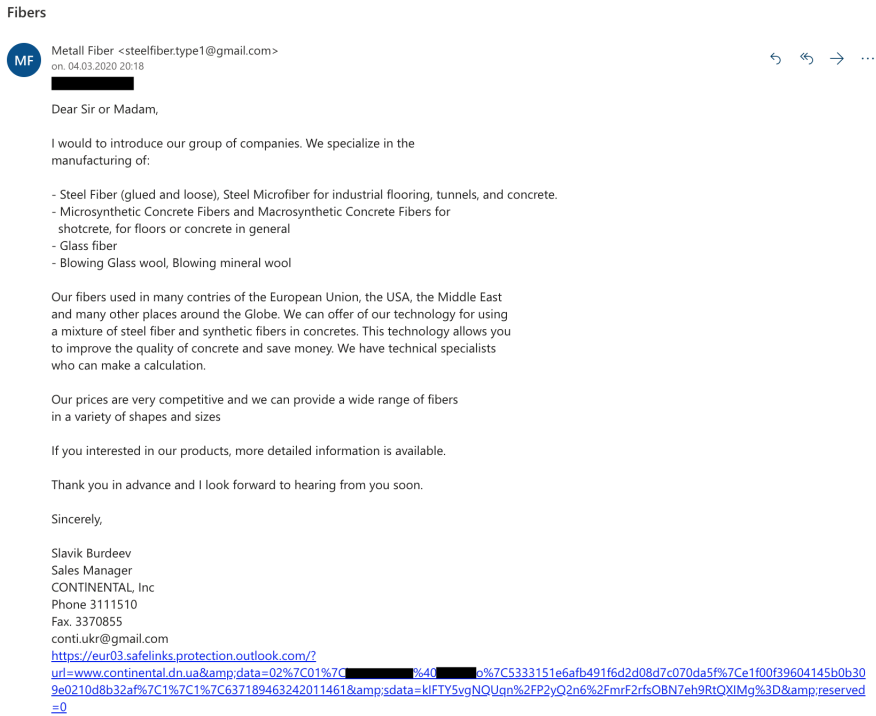
**Figure 4.10:** Email number 3 of the analysis of reported emails during the interviews. Received after implementation of the new security functions.

**Email 4 (figure 4.11)** In this email, where a company wants to sell metal fiber, there is a fully written and analyzed link. All of the seven asked employees say that they would have deleted or reported this email because the content is not relevant for them, and two statements from the interviewees are:

*"There is a long link in the bottom. If glass fiber were interesting for me, I would rather type in "Continental ink" in a web browser because that is the company name."*

*"I would not have clicked this link, mostly because I don't understand what it would have given me, and it is not something I have interest in anyway."*

One of the other interviewees were first asked if they would click the link if the product were interesting, and the answer was:



**Figure 4.11:** Email number 4 of the analysis of reported emails during the interviews. Received after implementation of the new security functions.

*"No, because I could have thought that it is a fraud, I would have googled the company first."*

Next, the interviewee was asked if it is hard to interpret the link, and the response was:

*"Yes, the first thing I see is "safelinks". If it hadn't been this kind of email, but from a company I have bought something from and they had sent me an email, I would have clicked it. I only see "safelinks" and think that it is good."*

Another of the interviewees think the link is hard to assess, and when asked if they would trust it because it is an analyzed link or if they would do more research they answer this:

*"I would have checked out "contintal.un.da" but in this case it doesn't affect me. If it was someone I know that knows me I would have asked for more information."*

Finally, another employee that is asked if it is hard to evaluate the link answers this:

*"No, it is just to look for the url= part. And then it is good that if someone clicks it, you are protected by safelink."*

**Email 5 (figure 4.12)** This is a short email from before the implementation of the new security solution that analyze links. All interviewees quickly conclude that the email is malicious. Sender, content, language and the link are factors that are mentioned. One interviewee will not click the link because it is not an analyzed link. One maybe could have clicked the link if the sender was familiar. Another one checks if the shown link is the same as the link shown on mouse-over, and because it is, the person assumes that they are phishing for a password and deletes the email.

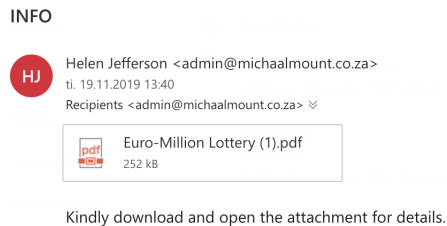


**Figure 4.12:** Email number 5 of the analysis of reported emails during the interviews. Received before implementation of the new security functions.

**Email 6 (figure 4.13)** All interviewees think it is easy to see that the sixth email is an attempt on fraud. That is mainly because of the name of the attachment. One of the interviewees says:

*"If this looked like a research paper from one of my colleagues, I think I would have opened it. Don't need much text either."*

There is a disagreement on whether there is a need for more text or not for the email to be trustworthy. One more of the employees support that there is no need for more text as long as the email is expected and the file has a serious name. Two other interviewees specify the need for more text for the email not to be suspicious. Alternatively, no text is better than one sentence if it is an expected document.

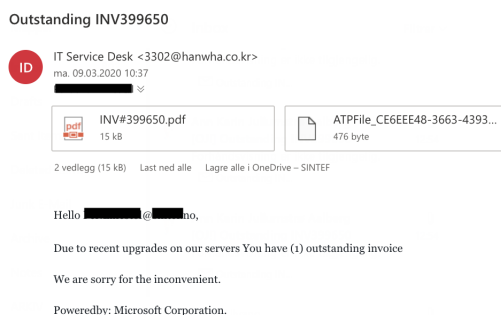


**Figure 4.13:** Email number 6 of the analysis of reported emails during the interviews. Received before implementation of the new security functions.

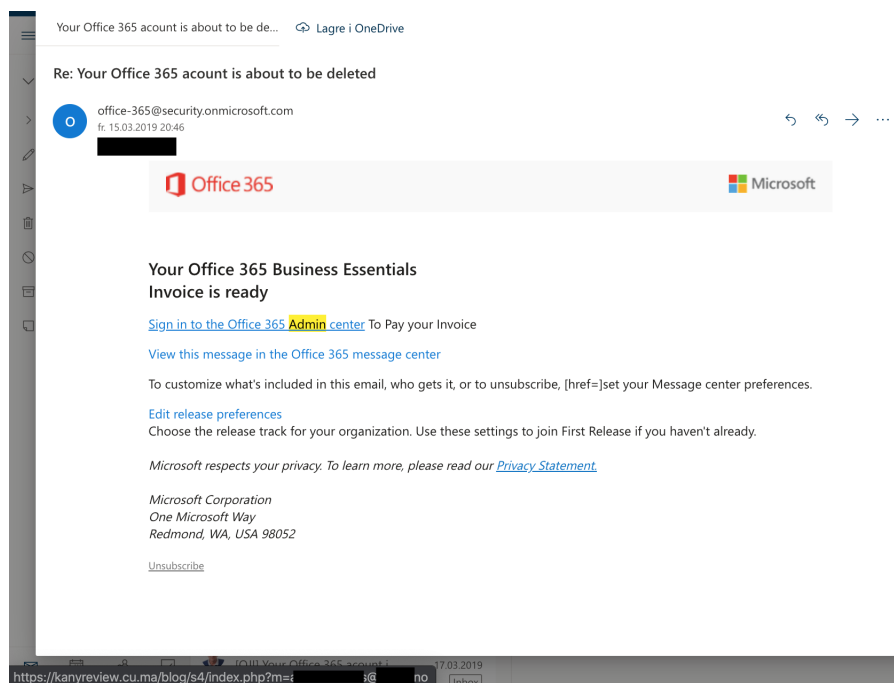
**Email 7 (figure 4.14)** All interviewees find this email suspicious because of sender and content. They were asked which role the other file called "ATPFile" has in their analysis, and no one says that it helps their evaluation. Three of the participants say that they never or rarely open those small files. None of the participants know exactly why it is there, and three think it is a small file for a company logo. One of the other interviewees say:

*"It doesn't help for the trustworthiness. In this case, they try to make it look like the protection thing from Microsoft, but they doesn't look exactly like that."*

**Email 8 (figure 4.15)** This email is from before the implementation of the new security solution, and the sender wants it to look like Microsoft sent it. All of the interviewees reveal that this is malicious, and five say that it is because it is not their responsibility to do any administration on their Microsoft account. None of them find it necessary to investigate the link, because they dismiss the email because of



**Figure 4.14:** Email number 7 of the analysis of reported emails during the interviews. Received after implementation of the new security functions.



**Figure 4.15:** Email number 8 of the analysis of reported emails during the interviews. Received before implementation of the new security functions.

other factors like expectation and title. For this email, only one of the interviewees mentioned the sender's email address as suspicious. One of the interviewees thinks this email looks quite real and says this:



*"This one is more tricky, the email address can be real. It is weird that the subject field contains RE since it indicates that I have a dialogue with them."*

Further, the interviewee is asked if they would use mouse-over on the link for evaluation, and the answer was:

*"Yes, maybe, it looks like spam. If it was sent to my private email it would seem more real, since you are not updating things like this yourself in an organization. Now I wouldn't click, but maybe five years ago."*

**Email 9 (figure 4.16) and 10 (figure 4.17)** These two emails are identical, except for that email 9 is from before implementing analysis of links and email 10 is from after the implementation. This can be seen when using mouse-over on the links. Out of six asked participants, five of them mentioned the sender's address as being suspicious. The last one says that they delete it because of not owning any Apple products. One of the interviewees answers this when analyzing email 9:

*"I received this, and my first thought was that the price was really increased. Then I saw the sender and that it is wrong. And then it is to check the log in link, and this is one example of that it looks nice graphically, but I can't assess the links when it is presented in that way. "*

Regarding the difference between email 9 and email 10, one of the interviewees says:

*"It doesn't matter that the link is shorter, the sender address is enough for me to ignore this email."*

One of the other participants say this:

*"It is clearly shorter in the first email, but when I have gone to the step where I use mouse-over, I would have looked at the content of the link, and it is just to get to know that you can look at the url= part."*

Another interviewee says this about the link in email 10:

*"Oh, there it is a safelink, then I maybe would have clicked, but not if it was from a weird address."*



# Chapter 5

## Discussion

In this chapter the results presented in chapter 4 will be discussed in light of the presented theory and background information from chapter 2. The discussion aims at answering the research question by discussing the defined sub-questions separately. Together with this, the implications drawn from the answers to the sub-questions are the answer to the research question. First, the sub-questions are discussed in section 5.1 and 5.2, before the implications in section 5.3. Section 5.4 presents possible limitations to the research that can affect the conclusion and suggestions for further work are presented in section 5.5.

As presented in the introductory chapter the research question is:

How are the user experience and the users' security awareness affected when security solutions for email develop from traditional signature analysis to automatic analysis based on machine learning algorithms?

Even before implementing the new security solution, information security was a big focus in the case organization. They were having security campaigns, where one of the main focuses is email security. Also, their security department always aims to improve security and are looking for new solutions. Therefore they chose to implement a SIEM platform where an email security solution with an advanced analysis of links is a prominent part.

The results indicate that this implementation has been well received on a general basis among the employees. However, there are some divisions as some of the interviewees think the analyzed links are easier to assess and others think it is harder than the original links. The data also suggests that already from before the implementation, there was a high degree of risk perception among the interview objects.

## **5.1 SQ1: How is the user experience intended to change with the new security solutions and how is the users' actual experience?**

Both the intentions of the new solutions and the actual experience are parts of this sub-question. The intentions when implementing the new solution in the case organization is already presented in section 4.1 in chapter 4, since the conversation with the security manager in the case organization gave answers to this part of the sub-question. The intentions are considered as realities from the case organization and are not a topic that needs much discussion. However, an overview of the case organization's intentions of the new solution is given, and then the actual user experience is discussed and compared to the intentions.

### **5.1.1 Intentions of implementing a new security system**

In general, when implementing new security solutions, the intention is to make the organization more secure. The current shortages in the organization form the basis for which solutions they choose. The needs are, among other things, affected by their current security situation and what goals they have for security. The knowledge and interests of their employees can also be factors in the choice of solution.

Before implementing the new system, the case organization predicted potential benefits and disadvantages with a SIEM solution. Their need was to respond faster and better to security incidents by getting a better overview of the incidents. For this, a solution that collects information from all their systems and uses advanced algorithms are suitable. Another benefit is that the response to an incident can be targeted against the device that might be infected and that the end user gets more control of the situation. The disadvantages with the new solution are that it requires more knowledge about the users and that therefore all information is connected by the system, which might be a problem if the information ends up in the wrong hands.

When implementing the solution, one purpose was to make the user satisfied by increasing security. For the user, the system should also be easier to use and therefore increase the user experience. Besides, the goal is to reduce the number of human errors by supporting the users in the utilization of the system. The system is not fully automated, and it is essential to remember that the user still has to make some choices; therefore, they want a system that is designed for the user to make the most secure choices. This is done by supporting the users in the evaluation of links in the system the case organization has implemented. In addition, the fact that the end user now has increased control can also affect the user experience.

### 5.1.2 Actual user experience

For the solution to be secure, it has to help minimize human errors, meaning that a well developed HCI can help to increase both usability and security. This is stated by Johnston et al. [JEL03], which has defined HCI-S with six criteria presented in table 2.3.1. When looking at the email security solution the case organization has implemented with the new presentation of links, it is possible to perform a small analysis of the new function with these criteria. The interface conveys security features to the user since the link now has a prefix saying "safelink". This is not a very direct way of doing it, but the wording indicates that there are security measures. Regarding the second criterion, the system shows the status if, for example, an attachment is being analyzed. The third criterion is harder to evaluate because it is individual whether the system feels non-threatening and is easy to learn. The interviews showed that there are differences in the understanding of how secure the system is to use among the employees, which can indicate that it is not very easy to learn for everyone. There are no indications that too much security information is displayed to the user. Error messages are not relevant to this. The last criterion about a satisfactory experience with the system seems to be fulfilled to some degree. The interviewees are satisfied at many points, but also have some suggestions to make it even better. All this indicates that according to the criteria by Johnston et al. [JEL03] the solution should give a good user experience with a few exceptions.

It seems like the users quickly discover the change in the presentation of links. The interview results shows that five out of seven participants mention the change in the presentation of links before being asking about it, and the last one tells about this change when helped a little bit. Because there is a detectable change, there is also a possibility for a change in user experience and usability.

One factor affecting the user experience is whether the user thinks the new links are easier or harder to evaluate. According to the definition of user experience by ISO [ISO18], the user's comfort, behaviors and accomplishments are part of the user experience. In our context, if the new presentation of links decreases the user's comfort, behaviors or accomplishments through the use of the email service, the user experience might also decrease. During the interviews, four of the seven participants find the links harder to evaluate now, two find it easier and one thinks it is no difference. This finding exposes different opinions in the case organization but indicates that the majority think the new presentation makes the evaluation harder. The fourth email the interviewees evaluated (figure 4.11) included an analyzed and rewritten link, and it is an example of how different the employees interpret the new links. When the evaluation is more laborious, it might be more challenging to accomplish the task, which is to understand whether the link is harmless or malicious. If the user cannot evaluate a link themselves, it can affect the behavior, and if they

do something they should not, it can affect their comfort. Their comfort can also be affected by the uncertainty in the situation because they do not know where the links lead to and that they have to spend more time investigating it. For the one that now finds the links easier to evaluate, the user experience might increase because of increased comfort and accomplishment. Because the majority of the asked in the case organization think the evaluation is harder now, we assume that this is a factor that decreases the user experience on a general basis.

A different perspective is that the user experience increases because the system already has evaluated the link on behalf of the user. Through the analysis of emails in the interviews, one of the participants said that when seeing the known prefix of an analyzed link, there is no need for more analysis of the link. The same person, along with another participant, also express this through the rest of the interview. When this is the case, the evaluation is much faster for the user, and the user experience may increase as a consequence of increased comfort [ISO18]. Even though this was only two of seven participants, it might count for other employees in the case organization or other organizations.

In addition to the possibility of analyzing the changed links themselves, there are other aspects with the links that might affect the user experience. On the positive side, it is a technical tool that takes some responsibilities from the user and might be more trustworthy. There were also mentioned some disadvantages directly with the functioning of the links. The employees have experienced problems with forwarding emails with expanded links and the expanded links are harder to read on the phone with a small screen. These are factors that decrease the user experience because the comfort of using the system is decreased [ISO18].

Advanced analysis of attachments is also a part of the new solution, but the users have not noticed it to the same degree as with the links. None of the interviewees mentioned it during the interviews, and through their analysis of the sixth and seventh emails (figure 4.13 and 4.14), it is clear that it does not matter for their evaluation. This might be because there has been more focus on the analysis of links in the case organization. Since the employees do not notice the analysis of attachments, it is reasonable to assume that it is not something that affects their user experience significantly.

The definition of user experience [ISO18] also includes the system's performance as one factor for satisfaction. If more of the email security solution than just the presentation of links are considered, one measure of the system's performance is the filtering of junk email. All interviewees were satisfied with this filtering, which implies that the employees are satisfied and it adds to increasing the user experience of the email system. Another measure of the system's performance is whether or

### 5.1. SQ1: HOW IS THE USER EXPERIENCE INTENDED TO CHANGE WITH THE NEW SECURITY SOLUTIONS AND HOW IS THE USERS' ACTUAL EXPERIENCE?

65

not the system correctly analyzes the links. If the user still receives many emails with malicious URLs, they will not be satisfied. Because of the way the system is designed, there is still a possibility that a user receives a malicious URL, but the possibility is decreased from before implementing the new system. However, some of the employees think that all URLs they receive are safe, and they are probably more satisfied than the others until an incident happens. Generally, there is an increase in performance with the new system, but it is not perfect.

From the inbox with reported emails, it is clear that there are still many emails that the users receive that they do not want, which implies a more unsatisfactory performance than what the interviewees said. Because of that, the user experience might be less increased than previously assumed. The inbox is for emails the users find suspicious, so it is conflicting that they are pleased with the filtering, but still are reporting this amount of emails. It may be because many report emails they receive in their junk inbox, which is also confirmed by some of the interviewees. One problem with using the amount of reported email as a measure for the user experience is that some employees might have difficulties distinguish malicious or other unwanted and commercial emails they have signed up for.

#### 5.1.3 Perceptions of protection of privacy and trust in the solution

In addition to the system performance and the interaction with the system, how the user trusts the system and their perception of protection of their privacy also affects the user experience [SHF<sup>+</sup>15][JEL03].

Regarding the protection of their privacy through the use of the email solution, all interviewees are okay with it, mainly because it is in work setting and that they do not have anything to hide. This implies that the culture in the organization involves accepting this privacy offer for the organization's security. There is neither anything that indicates that this was different before implementing the new security solution. Because privacy protection is not an issue, it is not a factor in affecting the user experience either [BSSU05][SHF<sup>+</sup>15]. Nevertheless, it is crucial to notice that only three of the interviewees are aware that the email security solution needs insight into their emails to do the analysis. During the interviews, the necessary data sharing was shortly explained to the ones who were not aware, so that they should be able to answer the question. The fact that they received this information during the interview can have affected their answers because they might not have had the time to reflect on it.

Seckler et al. state that lack of privacy increases distrust [SHF<sup>+</sup>15], so the high degree of perceived privacy protection in this case, should indicate a high degree of

trust in the solution or at least not contribute to distrust. However, there are also other factors that affect trust, and these are discussed in the next paragraphs.

Through the interviews, six out of seven participants say they trust the email security solution implemented in their organization. These answers indicate a generally high degree of trust in the solution through the whole organization. However, the trust can be in different parts of the solution, meaning it can be in the solution as a whole, in the filtering or directly in the links. The trust can also be established because of different reasons. Some of the interviewed persons trust the system because of its performance and some because they trust that the IT department in the organization takes the correct decisions.

Research, e.g. [SHF<sup>+</sup>15] and [JEL03], shows that trust is important for a good user experience. The results from the interviews indicate a high degree of trust in the solution among the employees in the case organization, which can imply a good user experience. However, the effect trust has on user experience might vary depending on the reason for trust. It is reasonable to assume that the people who trust the system because of its performance have a satisfying user experience because their trust is directly in the system. On the other hand, the employees who trust the system because they trust the IT department may not have the same effect on user experience. There is also one interviewee that says that *they just have to trust the system*, which indicates that their behavior is the same as if they trusted the system. However, this kind of trust is not consistent with the definition of trust, which specifies that it should be a firm belief [oxf15]. This attitude might count for several employees and is probably not contributing to increasing the user experience.

Another thing to consider when evaluating the effect of trust on user experience with the new system is whether the degree of trust is something that has changed with the new system. Two of the interviewees fully trust the analyzed links, which means they have increased trust in email links with the new system and it is, therefore, an observable change with the new system. The analysis we performed in the previous section of the HCI-S using Johnston et al. criteria also indicates an increased trust [JEL03]. On the other hand, the trust of the people who rely on the IT department choices is probably not affected by the change. Among the people that trust the system directly, some justify this trust with the high performance of the filtering. None of the interviewees had recognized any significant difference in this filtering, and, therefore, the ones that have the high performance of filtering as a reason for trust may not have changed their trust in the solution with the changes.

Regarding the trust in the analyzed link, one hypothesis is that because of its complex design the users find them more suspicious. This hypothesis is based on research by Jakobsson et al. [JTS<sup>+</sup>07] who found that syntactically different URLs



are often suspected to be malicious. This is not the case with the new presentation of links, because no one expresses that they have less trust in the links now and more often suspect the links to be malicious. The situation with the complex URLs in the email solution that is studied in this project is a little different since they are all rewritten and the reason for doing it is security. Because of this, everyone knows how the links are supposed to look. At the same time, this means that the user loses the opportunity to quickly decide if the link is syntactically different because all links are lengthy and complicated.

Through the literature study, there was identified a gap in the research about trust and privacy in email security solutions. Our research shows that at least in the case organization, the trust in the email security solution is high among the employees and that this has various reasons. Because of the clear indications, it is likely to assume that this counts for users in general. What mainly affects the trust is the perception that their privacy is protected or that the lack of privacy is necessary and useful, as well as observing that the system has a good performance. These results are a star to filling the identified gap, but more research is needed.

To summarize the discussion around the first sub-question, we have seen that the employees' experience with the new security system is divided, but the majority think the rewritten links are harder to evaluate themselves. However, because someone thinks the new links are easier to interpret and everyone thinks the filtering is working well, there are also improvements to the experience. There is a high degree of trust in the solution, which adds to an increased user experience. To the extent that this can be interpreted from the available data, it seems that the user experience, in general, is slightly increased. The intentions for the case organization was an increase in user experience, and this is fulfilled to some degree, but their intentions probably was an even more significant increase.

## **5.2 SQ2: How does this new user experience affect the users' security awareness?**

This new user experience contains several elements, including the new presentation of links and how they experience the filtering. The question says *new* user experience, but there might be some elements that are the same as before and that will be considered in the following discussion. As noticed in chapter 2, there is a lack of research on how a change in user experience affects security, but it is interesting to see whether there are any parts of the new solution that affects this. For the investigation, there is first an analysis of the employee's perception of the threat landscape, which can say something about their risk perception. Then to understand more about the security awareness among the employees, we discuss how they avoid

email threats, if what they say that they do is what they actually do and which other factors that influence the security awareness.

### **5.2.1 The employees' perception of risks and threats**

To understand how the risk perception changes when new systems are introduced, it is interesting to look at the user's perception of the threat landscape they are exposed to. Risk perception is about both beliefs and actions [Slo87], and through the interview, their thoughts about risks were identified. It was clear from the interviews that all participants are aware of the threats their organization is exposed to through email and that they have a responsibility when utilizing the email system. This indicates a high degree of risk perception among the employees in the case organization. The high degree of risk perception is also supported by the study by NorSIS from 2016, which shows that most people think they are exposed to risk when they are online [MR16].

A person's risk perception is affected by many factors [Slo87], so it is hard to tell how much effect the new security system alone has. Most of the focus among the interview objects was on the threat that they receive something damaging that leads to monetary loss, loss of reputation, loss of secret information or revealing personal data. They also gave examples of incidents where such things have happened. These threats are probably not something that has changed significantly with the implementation of new systems. Other factors like incidents in the news or information from the IT department might have more prominent effects. Also, if the new system led to significantly increased risk perception, the number of reported emails might have increased since the employees did not discover any changes in the spam filtering. The analysis of reported emails does not show any significant differences, so this implies that there is no difference in risk perception with the new system. It is hard to be confident that there is no difference now, and more research is needed to be able to conclude.

Even though the employees have a high degree of risk perception, they might lack knowledge, which potentially can lead to dangerous situations. One example of this is that all interviewees understand that links and attachments provide a risk. However, they are not aware of what kind of attachments that can be malicious. One interviewee said that the attachment had to be an executable to be dangerous, which is not correct as office files are the most normal malicious attachment [Sym19][Ver19].

### **5.2.2 How the employees avoid email threats**

It was evident during the interviews that the most important tool the employees use to avoid threats is to evaluate the emails they receive. How the employees evaluate an email says something about their security awareness. Generally, all the employees

that are interviewed have routines to check the emails they receive to detect if it is something suspicious or if the email can be trusted. This result confirms that there is a high degree of risk perception among the employees and that they have the ability to utilize it in practice as well.

The most important factor they use for evaluation is whether or not the email is expected. This is confirmed both through conversation during interviews and the analysis of emails the participants did. Therefore the risk increases when an attacker imitates an email the receiver expects. The new system might not be as good at filtering out these kinds of emails as the general spam emails, which poses a risk. In itself, this does not imply a higher risk than with the old system, but the problem is if the users now receive less general spam and because of that lower their guard. This might lead to malicious emails that look like expected emails and are not detected by the system, are not detected by the receiver either. The threat report from NorSIS shows that the amount of targeted and personalized attacks is increasing [Nor20], which increases the risk of using this filter as the primary evaluation method. The technology the attackers have available makes these kinds of emails continuously better, which means that the users now should be even more guarded.

When asked how to escape the email threats, all the interview participants seem to know that they have to avoid clicking malicious links and opening malicious attachments. However, it does not seem like that to look at the syntax of the links directly is an essential part of their email analysis. The impression is that they instead use the context for evaluation, including whether the sender and sender's address are coherent, the language and email headers. This result does not fit with the research by Jakobsson et al. [JTS<sup>+</sup>07] who found that the URL is an important part of the analysis of a web page or email. However, from the analysis the participants did of the emails they were presented for, it seems like there is more focus on the link than they are saying. This might be affected by the earlier part of the interview, but might also indicate that the URL is one of the factors the employees use for evaluation. The significance of the URL is vital because it says something about how important the new solution is and its effects. We can conclude that other factors are more critical for the evaluation, but that for some employees, the syntax of the URL also is important for the evaluation.

Another interesting thing to mark from Jakobsson et al. [JTS<sup>+</sup>07] research is that they found that faux-personalization creates trust and could, therefore, be a part of an email evaluation. This is not something that the employees in the case organization explicitly mentioned, but during the analysis of reported emails, some find it suspicious when the email starts with their name, especially the email address. On the other side, a faux-personalization can make the email seem more personal and directed, and therefore maybe seem more expected, which is a filter the employees use

frequently. To judge relevance before authenticity was also presented by Jakobsson et al. [JTS<sup>+</sup>07] as a filter for trustworthiness, but not mentioned directly by the interview objects in our study. The participants have a big focus on expectation and thereby also relevance, but at the same time, they are concerned to check the sender's address. Therefore it is difficult to say what is more important of relevance and authenticity for the employees in the case organization. There are differences between our findings and Jakobsson et al. [JTS<sup>+</sup>07] findings, and there are some similarities. The differences might be because the research by Jakobsson et al. [JTS<sup>+</sup>07] is from 2007, or can be because of other circumstances. However, it is interesting to note that this might have changed the last years as a consequence of technological development.

### 5.2.3 Are their behavior consistent with what they say?

It is not enough that the employees have fear and understanding of cyber incidents to change security behavior [ENI19a]. So even though the employees have a good perception of the potential threats, it does not necessarily imply that their behavior corresponds to this perception. In our case, the main behavior to change is how to evaluate a link and decide whether to click it. If the users do not change the behavior, the improved system will not be fully utilized. For some of the employees, we have seen that this behavior is slightly changed. Other employees might also change the behavior with time [ENI19a].

Even though the employees are saying that they carefully analyze and evaluate the risk of the emails they receive, the results from the phishing test fall 2019 give a different impression (figure 4.1 and 4.2). In the first 24 hours after sending out the email, almost 20% clicked the link in the email. The email was well designed to look like an internal email, but some hints should reveal the phishing if carefully checking the email. One of these things is slight changes in the sender address, which all say that they are checking when receiving an email. These results imply that even though the employees show security aware behavior, there might be trouble if the malicious email is targeted directly against a person or the organization and also is well designed. When 20% click the link in this test, the probability is significant that someone will be tricked by a well designed malicious email.

Research by Bada et al. [BSN19] shows that correct answers does not mean that the individual is motivated to behave according to the knowledge gained during an awareness program. This can explain the finding that the employees' behavior is inconsistent with what they answer during the interviews. Through the case organization's awareness program, they have learned how to evaluate emails they receive, but these findings might indicate that they do not have the motivation to do so. It can also indicate that they lack coping skills because that has a strong connection to security behavior [ENI19a]. Time limitation is also a possible factor

because even though they know how to perform security tasks, they do not take the time. This is supported by the research by Edwards et al. [EPS08], which hesitates that for the employee to perform the security tasks, it can not be an obstacle in work with their primary tasks. This can explain the inconsistency between what they say and what they do because even though they know what to do, the obstacle might be too big. It might be that since this phishing test was quite similar to an original email, the obstacle is more prominent because it requires more work to detect than with regular spam emails.

One can argue that in the analysis of emails during the interviews, the participants showed the opposite behavior of what they did in the phishing test because they all were able to analyze these emails correctly. This shows even more that they know what to do and look for. During the interviews, they do not have the obstacles in motivation and time limitations, so it is hard to compare with what they do in real life.

It is important to note that in this test, some people are clicking the link because they understand that it is fake, which gives a misleading number. However, since the number of clicks is high, it is likely that this does not count for all of the clicks and that there are still many that did not detect the phishing. There might also be people not having the time to open the email before it was revealed, which misleads the number in the other direction.

One of the interviewees admitted that he had clicked the link because he thought it was real:

*"They were smart because they sent it out early in the evening, so I received it on my phone, and then I am less observant. It was just a short time after I started here, so I hadn't received it previously and didn't know how it is supposed to look"*

It is remarkable what is said about not knowing what the internal emails are supposed to look like, which shows that new employees might pose a more significant risk to targeted emails that are imitating regular and internal emails. Even though the system is becoming better, if an email like that passes through the filter, it can be hard for a new employee to detect it with their human filter.

#### **5.2.4 Effects on security awareness**

We have seen that the users are affected by the implementation of the new system, but it does not seem like their security awareness is directly affected by the new functions. The careful procedure for evaluating emails indicates a security behavior

that existed before implementing the new solution. The main change in the security solution for email that we have studied is an analysis and new presentation of links, and the majority of employees have noticed this. However, the URL is not a very prominent part of the employees' evaluation, which might indicate that the change in email security solution we are studying does not directly affect security awareness.

Even though the new function does not have a direct effect on security awareness, the users might be affected by the complete system. As pointed out by one of the interviewees, the fact that it is a system behind can have a positive effect on security awareness. The change in presentation of links can work as a constant reminder that it is security mechanisms in behind, and maybe remind the user of why it is necessary. This can increase security awareness.

The trust in the solution affects the user experience, and it might also affect security awareness. Most employees trust the security solution and some fully trust the analyzed links. Some of the participants are not able to analyze the links themselves anymore and feel that they have no other choice than to trust the system. This can indicate a decrease in security awareness among this group of employees because they do not take responsibility for their actions and do not know that the analyzed links can be insecure [BCB10]. It is also a disclaim of responsibility because someone now says that it is the system's responsibility to make sure we do not click a malicious link. Some of the interviewees express that it feels good to have a system for this reason.

Change in security awareness among the employees is not only a consequence of the new security solution. Other things can have possible significant effects and it is impossible to isolate and only look at the effects of the new solution. This is confirmed through the analysis of the inbox with reported emails, which shows waves of emails in some periods. Such periods can be triggered by events like phishing campaigns in the case organization or big happenings regarding cyber security in media.

The discussion around this second sub-question has investigated how security awareness is affected by the new security solution. It is clear that the employees' risk perception is high, but we did not find anything that indicates that this definitely is because of the new system. However, there are changes in the new system that might have affected security awareness. In total, our results indicate that there are individual differences between the employees for security awareness and that someone might be affected in a negative way and others positively.

## 5.3 Implications

The two main elements of the research question, user experience and security awareness, have been discussed in the two sub-questions. This section provides the implications of these with reflections around the findings by discussing if the system makes an organization more secure and whether there are something that can increase the security even more.

### 5.3.1 Is the organization more secure now?

For an organization to be more secure, the risks should be reduced and the amount of threats decreased. This is achieved through implementing countermeasures, like the new security solution for email. As the background information about the email threat landscape showed (section 2.1), the main threats are the insider threat and to receive and interact with something malicious. Therefore, whether these threats are reduced can be used as a measure of security.

The interviewees are split between completely trusting the analyzed links and not trusting them at all, which indicates that they have not received the same information or that there is a lack of information on this point. Wang and Emurian [WE05] conclude, among other things, that even when an interface is created to induce trust, the consumer will still have to be informed about present risks and protections. Through the conversation with the security manager, we learn that the links that appear as safelinks not necessary are safe to click. This means that there is a risk because not all users are aware of this, so their security awareness regarding the links will be different. This is an example of the importance of education when implementing new systems so that all are aware of how it works to get the full effect.

This finding is also consistent with the finding of Bulgurcu et al. [BCB10] who found that for an organization to benefit from having an ISP the users have to be educated. A security system is not the same as an ISP, but to use the system correctly can be a part of the ISP or we can assume that the same counts for the use of a system from what we have found in this project. On the other hand, one can argue that the reports by ENISA [ENI19a] and NorSIS [MR16] say the opposite; that education will not help. However, these results are interpreted to count for education in information security that aims to increase fear, but the identified need for knowledge is about the functioning of the system. Therefore, such education must be focused on increasing knowledge and giving information about what the system protects the user from, but also the system's weaknesses. This kind of education is supported by the research by Downs et al. [DHC07], who found that the ability to parse URLs is important to be able to detect phishing attempts. They also support that increasing the fear of consequences is unnecessary and will only lead to more false alarms.

Edwards et al. [EPS08] identified the need for more research on the non-technical constraints of security, and we see that users misinterpreting the function of the systems can be a non-technical constraint that decreases the security gains of the new technology we are studying. The implemented solution can be looked at as a STS instead of a fully automated system, and therefore, users can affect the system's performance. The problem with this is that many users do not have security as their primary tasks [EPS08], and give it less priority. For example, a couple of the interviewees mentioned that they sometimes do not have the time to check the emails very carefully. When the system is depending on the user to be entirely secure, it might not be as secure as using a fully automated system. However, the feeling that some users have that the system is fully automated can be dangerous because it removes the human filter leading to potentially threatening situations.

Flechais et al. [FRS05] emphasize that a countermeasure has to be both correct and dependable. Measures of the system, presented in figure 4.4, shows that malware is detected, which indicates correctness. The graph does not say what is not caught by the system, but there is nothing that indicates that there is a lot that goes through. The dependability is affected by the users and how they utilize the system. The fact that not all employees are aware of how the system works and, therefore, make wrong choices affects the system's dependability negatively. It can also be affected if the employees do not have the motivation to use the system correctly. If the system's dependability is weakened, so is the security in the organization [FRS05].

A threat to the organization's security that is still important to consider is when attackers imitate emails that the user expects. This threatens both the correctness and the dependability of the system. The correctness is threatened because the system might not be able to filter out malicious emails that are targeted and unique. The same counts for dependability because the human filter is weaker in such cases. If both the correctness and dependability of the system is threatened, so is the organization's security [FRS05].

There might be that some of the others in the organization are in more need of the implemented security solution than the employees we have interviewed. One of the interviewees says that he thinks the organization in total is better equipped even though he is not affected very much. This suggests that the security is improved with the system because he probably knows his colleagues and their abilities, and see that someone is more in need of a solution like this than he and the other interviewees. At the extreme, we can state that it is enough that one employee makes better decisions with the new solutions for the organization to be more secure.

As the threat landscape indicates, one of the biggest threats is the unintentional insider threat, so if the insider threat is decreased, the security should increase. One



way this threat could be decreased is if there are fewer possibilities for human errors, such as a user clicking a malicious link by accident. Since the filtering is improved with the new algorithms and the employees are experiencing small amounts of spam in their inbox, there should be fewer opportunities to click a malicious link. Our results indicate that it can make the users less conscious, but that the consistency in a technical tool weighs out this disadvantage. Also, if there are employees that now are more security aware they are less likely to misinterpret a malicious email and interact with it. This contributes to that the insider threat is decreased with the implementation of the new systems.

### 5.3.2 Suggestions for improving the security solution

Since the solution does not make the security or the user experience perfect, there is still room for improvement. New functions can be implemented by taking advantage of the advanced technology already there to expand the email security solution. There are also measures to increase the security awareness that is outside of the concrete solution, including more education.

One thing that can be added is a categorizing of emails that are visible to the user. This suggestion was proposed by two of the interviewees. The system is already performing an internal categorizing, so implementing this in the user interface will increase the transparency. This function will add to the visibility of system status to the user, which is the second criteria in table 2.3.1. The user gets more insight into the internal security operations and, therefore, can increase user experience and trust [JEL03]. On the other hand, there is a risk that it can be confusing for the user with this information because it might not be correct or cause an overload of information. An overload of information can be harmful to the usability of the system because it decreases the simplicity [Nie94], so before implementing this function there is a need for more investigation on the positive effects versus the adverse outcomes.

A big part of the organization's security is the employees' filters, so adding functioning to help human filtering can increase security. One interviewee suggested a warning sign on suspicious sender addresses. Then fake email addresses that are similar to real ones can be detected more easily by the users. For instance, the sender's address in the phishing email the case organization sent fall 2019, where there were only small changes to a known email address, could be easier to detect. The design of the warning has to be carefully chosen. For example, it is proven that active warning signs are more effective than passive [ECH08] and that exclamation mark is attractive among users [SZSS16]. The exact layout for the best effect on security and user experience in this case is a topic for future research.

Another improvement could be not to use the function for analysis of links on internal emails. The security manager said that they have tried to do that, but there

are some problems with the tuning of the system. If this is done, it might be easier to identify if there are sent out fake emails pretending to be regular internal emails. This could potentially avoid the case that new employees are more vulnerable to that type of malicious email because they could detect that the URL is strange.

## 5.4 Quality and limitations of the research

The results from this research might be affected by how the research was conducted with the chosen methods, and therefore the relevant limitations are discussed in this section. The quality of the research is also an essential factor, and three measures on the quality in research are generalizability, reliability and validity [Tjo10]. These measures are used to evaluate the quality of our research.

Reliability in the research can be affected by the researcher's interests in the field, and it is important to be aware of and explain how this can affect the research [Tjo10]. If another researcher were to conduct the same case study, the person should get the same findings and conclusions [Yin09]. The studied research topic is of interest to the researcher, and the researcher is educated on this topic but does not have any particular interest in the concrete systems. The researcher has no connection with the case organization from before the project. However, one threat to reliability can be the close cooperation the researcher has had with the case organization during the project, getting to know them and hearing their thoughts. Nevertheless, this close cooperation can also give less bias [Rob11]. Therefore this should not affect the reliability of the results and conclusion.

One problem might be that the research project only investigates the change in one organization because the project is carried out as a case study with one case. The research project aims to investigate a technological change that is affecting many organizations in different industries. Generalizability is essential for making the research relevant to other scenarios outside the case studied [Tjo10], so having only one case organization might decrease the possibility for external generalization [Rob11]. The research is designed for generalizability to overcome this obstacle by not making the concrete security solutions in the case organization the focus of the study. Instead, the technology behind the solution is in focus, which will be similar for more solutions. At the same time, there are always individual differences between organizations, because there are so many factors in the topics we are studying. The case organization has had a big focus on security awareness training in the last years; hence the results might be different for an organization without any security education. The organization is a knowledge organization and that might also affect the results because their security culture might be affected by being used to sharing their projects with the society. Therefore the results might be less valid for organizations in other kinds of industries.

Validity is the measure of whether the answers we get actually are the answers to the research questions. The validity can be strengthened by openness and explanation of decisions taken [Tjo10]. In this thesis report, the decisions taken regarding methodology are carefully presented in chapter 3 to increase validity. Generalizability is also a measure of validity [Yin09], and as seen, there are a couple of limitations on generalizability in this research, but they are considered throughout the study. The following paragraphs discuss other potential limitations in the validity of the research.

The case organization has approximately 2000 employees, but in this research project, only seven of them were interviewed. That is a small share and can be a threat to the internal generalization [Rob11]. All employees were invited to participate, and the seven interviewees are the ones who volunteered. Problems regarding this are presented earlier in the section about the recruitment of interview objects (section 3.6.1). The difficulties include the fact that it is impossible to know what the employees not interviewed think and what information is missing. If important information is missing, the validity is affected. At the same time, there is limited how much new information the next interviews will give because, at some point, information saturation is reached.

Another issue with having a small share of the employees and recruiting by having people volunteering is that there might be the the most interested in the research field that volunteer. Therefore, it might be that the employees participating in the interviews have different perspectives and opinions than a general employee. These people might also have more knowledge about information security than an average employee and therefore be more security aware. Only one of the seven participants admitted to having clicked the link in the phishing test from the case organization, which is the same as 14.3% of the participants. The results from the campaign show that after seven days, 28.1% of the employees have clicked the link. Comparing these percents indicates that the interviewees are over the average on security awareness in the organization. After having conducted the interviews, it is clear that some of them have a special interest in the field, but a couple of them just wanted to learn and help the research project. The interviewees are people with different backgrounds and from different departments, which increases the validity of the research. Besides, several methods for data collection are used to support the interview results, which also decreases the disadvantage of few interviewees.

The participants might not have been honest when answering the questions. This can be intentional, but it can also be unintentional. For example, it might be that although they say that they have good routines for evaluating received emails, they might not be that careful in practice. It is, therefore, crucial for the interviewer to reflect on whether the presented information is the interviewee's true opinions [Tjo10].

This is done by comparing the answers we get with behavior we see through the inbox with reported emails and responses to the phishing test.

Open questions were used because they increase the interviewee's opportunity to reflect and bring up new ideas [Rob11]. This can give the necessary input to the research problem. However, the open questions can make it harder to compare some of the answers, because they can be very different. It might be that some of the other interviewees think the same as the one who mentioned something but did not think about it during the interviews since they were not specifically asked about it. This makes it harder to compare the answers from the interviews directly, and it will be an uncertainty in the number when counting how many said the different things.

In this research, the goal is to investigate a change, so a limitation is that the research only is conducted after the new system is implemented. Change in behavior takes time [ENI19a], so the time limit of this project is a limitation in the conduction. Ideally, the research project should have a longer duration and started before the new system was implemented. In that way, it would have been possible to do interviews with the employees before and after the change, which probably would have given more insight into the employees' security awareness and the general security situation before the new systems. However, this was not possible due to time limitations. The change is investigated by looking at the reported emails, talking with the security manager about the security situation before the new systems and asking the interviewees about the change.

To summarize, there are possible limitations with this research project because it is only one case organization, the number of interviewees is small, the questions might be biased and it is hard to investigate a change when only looking at the afterward situation. At the same time, the quality measures are considered during the process and measures are done to ensure the highest possible quality within the project's natural limits.

## 5.5 Further work

Similar research can be performed in other organizations and industries to make the results more general. It would also be interesting to investigate other systems that rely on the change from traditional signature analysis to automatic analysis using machine learning.

The findings from this research project can also be used to find ways to adapt security training to the new systems, but exactly how to do it needs more research. It is, among other things, identified that lack of knowledge about the new technology could decrease the organization's security. More research is needed to confirm the

finding and figure out how to improve security training efficiently. It is also interesting to investigate deeper the interaction between information security and psychology. This includes to study differences between the ones who are security aware and those who are not. Are there any similarities between the people who becomes less security aware when improved technology is implemented? To know what creates these differences are important, and such knowledge can be used to improve the security training.

It would be interesting to know more about how new technology affects the potential threats. A more detailed analysis of the reported emails in the case organization would be interesting to compare with the results from Fagerland's master thesis from 2017 [Fag17]. It would also be interesting to investigate what kind of emails still passes the filter. That can potentially say even more about whether something has changed regarding what kind of threats the organization is exposed to through the use of email.



# Chapter 6

## Conclusion

New and technically better solutions are implemented to improve security, but it is a challenging balance to secure something while creating a satisfying user experience and preserving the users' security awareness. Our research aimed to identify the effect of new security solutions for email on user experience and security awareness. To make a conclusion that can say on a general basis whether the user experience is improved or reduced and whether or not the security awareness is increased are difficult because there is significant individual differences. However, some implications based on the collected data are made.

There is a change in user experience when the security solutions for email develop from traditional signature analysis to automatic analysis based on machine learning algorithms. The employees notice the change in links, but there are disagreements in whether the new presentation increases or decreases usability. The majority think the links are harder to evaluate now, which for someone gives a decrease in user experience, but for others it still increases the user experience because an analysis is performed. It is important to note that the link itself is not an essential part of the employees' analysis of emails, which decreases the effects of this new function. In addition, the general trend among all employees is that privacy is not a problem and the employees have trust in the solution. This adds to an improved user experience, together with the satisfaction of the system's filtering of spam.

As with the user experience, there are also individual differences in the security awareness among the employees. For someone, there is no notable change in security awareness, but for someone else, the security awareness might be decreased because they now fully trust the system's analysis. At the same time, someone gets increased security awareness because the security system constantly reminds them of the risk of using email. The employees have a high degree of perception of risks and threats they are exposed to through email. They have careful routines to check the emails they receive, but there are indications that they do not always perform this in practice. This, together with other things, implies that there are still human filters that can

fail and increase the risk for security incidents, which underlines the need for reliable security systems.

In total, it seems like the organization's security is slightly increased when implementing the new security solution, but there are indications of both increased and decreased security. Some of the employees have lowered their guard, which is a threat to security, while someone is more security aware because the system reminds them of the possible threats. Simultaneously, the system has improved the filtering, which leads to less possible interaction with malicious emails. Therefore, the unintentional insider threat is slightly decreased because of the shrinkage in the possibilities of human errors. However, emails that imitate expected emails still contribute a risk, because in many cases these are not detected by either the technical or human filter.

Our research contributes to filling the gap in the research on the interaction between user experience and security awareness. We have found that there is a need for more knowledge among the users, so the key takeaway to organizations implementing new security solutions is to make sure the user knows how to utilize the systems correctly. At the same time, the user must remember that even though there are new and improved systems, they still have to keep their human filter because a system will never be completely bulletproof. In the future, there is a need to do similar research with other systems and in other organizations and precisely identify how security training should be adapted to the new systems.



# References

- [BCB10] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Q.*, 34(3), September 2010. Available at: <http://dl.acm.org/citation.cfm?id=2017470.2017477>.
- [Bej04] R. Bejtlich. *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Pearson Education, 2004.
- [BSN19] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? *CoRR*, abs/1901.02672, 2019. Available at: <https://arxiv.org/abs/1901.02672>.
- [BSSU05] Yakov Bart, Venkatesh Shankar, Fareena Sultan, and Glen L. Urban. Are the drivers and role of online trust the same for all web sites and consumers? a large-scale exploratory empirical study. *Journal of Marketing*, 69(4):133–152, 2005. Available at: <https://doi.org/10.1509/jmkg.2005.69.4.133>.
- [CRC08] Patricia Cronin, Frances Ryan, and Michael Coughlan. Undertaking a literature review: A step-by-step approach. *British journal of nursing (Mark Allen Publishing)*, 17:38–43, 01 2008. Available at: <https://doi.org/10.12968/bjon.2008.17.1.28059>.
- [DHC07] Julie S. Downs, Mandy Holbrook, and Lorrie Faith Cranor. Behavioral response to phishing risk. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit*, eCrime '07, page 37–44, New York, NY, USA, 2007. Association for Computing Machinery. Available at: <https://dl.acm.org/doi/abs/10.1145/1299015.1299019>.
- [ECH08] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You’ve been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, page 1065–1074, New York, NY, USA, 2008. Association for Computing Machinery. Available at: <https://dl.acm.org/doi/10.1145/1357054.1357219>.
- [ENI19a] ENISA. Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. Technical report, ENISA, 04 2019. Available at: <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity>.

- [ENI19b] ENISA. Enisa threat landscape report 2018. Technical report, ENISA, 01 2019. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>.
- [EPS08] W. Keith Edwards, Erika Shehan Poole, and Jennifer Stoll. Security automation considered harmful? In *Proceedings of the 2007 Workshop on New Security Paradigms*, NSPW '07, page 33–42, New York, NY, USA, 2008. Association for Computing Machinery. Available at: <https://dl.acm.org/doi/abs/10.1145/1600176.1600182>.
- [Fag17] Vegard Fagerland. Automatic Analysis of Scam Emails. Master's thesis, Norwegian University of Science and Technology, 2017. Available at: <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2461337>.
- [FRS05] Ivan Flechais, Jens Riegelsberger, and M. Angela Sasse. Divide and conquer: The role of trust and assurance in the design of secure socio-technical systems. In *Proceedings of the 2005 Workshop on New Security Paradigms*, NSPW '05, page 33–41, New York, NY, USA, 2005. Association for Computing Machinery. Available at: <https://doi.org/10.1145/1146269.1146280>.
- [Gee04] Frank W. Geels. From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory. *Research Policy*, 33(6):897 – 920, 2004. Available at: <https://www.sciencedirect.com/science/article/pii/S0048733304000496>.
- [Har98] Chris Hart. *Doing a Literature Review: Releasing the Research Imagination*. Sage publications, 2018, 1998.
- [Hyd19] Hydro. Cyber-attack on hydro. <https://www.hydro.com/en/media/on-the-agenda/cyber-attack/>, 11 2019. Accessed: 2020-01-29.
- [IAP19] IAPP. What does privacy mean? <https://iapp.org/about/what-is-privacy/>, 2019. Accessed: 2020-03-02.
- [Int20] QSR International. Powerful research, simplified, 2020. Available at: <https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/about/nvivo>, Accessed: 2020-04-15.
- [ISO18] ISO. Ergonomics of human-system interaction — part 11: Usability: Definitions and concepts, 2018. Available at: <https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en>.
- [JEL03] J. Johnston, J.H.P. Eloff, and L. Labuschagne. Security and human computer interfaces. *Computers & Security*, 22(8):675 – 684, 2003. Available at: <http://www.sciencedirect.com/science/article/pii/S0167404803000063>.
- [JTS<sup>+</sup>07] Markus Jakobsson, Alex Tsow, Ankur Shah, Eli Blevis, and Youn-Kyung Lim. What instills trust? a qualitative study of phishing. In Sven Dietrich and Rachna Dhamija, editors, *Financial Cryptography and Data Security*, pages 356–361, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. Available at: [https://link.springer.com/chapter/10.1007/978-3-540-77366-5\\_32](https://link.springer.com/chapter/10.1007/978-3-540-77366-5_32).

- [Kin16] John Kindervag. No more chewy centers: The zero trust model of information security. *Forrester*, 1(1), March 2016. Available at: <http://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf>.
- [ML19] Jan M. Moberg and Kurt Lekanger. Offer for omfattende dataangrep – slik kan næringslivet ta forholdsregler. <https://www.digi.no/artikler/intervju-offer-for-omfattende-dataangrep-slik-kan-naeringslivet-ta-forholdsregler/477063>, 10 2019. Accessed: 2020-03-06.
- [MR16] Bjarte Malmedal and Hanne Eggen Røislien. Cybersecurity risk perception, 2016. Available at: <https://norsis.no/wp-content/uploads/2017/03/Risk-Perception.pdf>.
- [Nas19] Nasjonal Sikkerhetsmyndighet. Risiko 2019 krafttak for et sikrere norge. [https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm\\_risiko\\_2019\\_final\\_enkeltside.pdf](https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf), March 2019.
- [Nie93] Jakob Nielsen. *Usability Engineering*. Academic Press, 1993.
- [Nie94] Jakob Nielsen. Enhancing the explanatory power of usability heuristics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '94*, page 152–158, New York, NY, USA, 1994. Association for Computing Machinery. Available at: <https://dl.acm.org/doi/10.1145/191666.191729>.
- [Nor20] NorSIS. Få en tryggere digital hverdag: Trusler og trender 2019-2020. Technical report, NorSIS, February 2020. Available at: <https://norsis.no/trusler-og-trender-2019-2020/>.
- [oxf15] Oxford english dictionary, 12 2015.
- [PST20] PST. Nasjonal trusselvurdering 2020, 02 2020. Available at: [https://pst.no/globalassets/artikler/utgivelser/2020/pst\\_trusselvurdering\\_2020.pdf](https://pst.no/globalassets/artikler/utgivelser/2020/pst_trusselvurdering_2020.pdf).
- [Ran09] Justus Randolph. A guide to writing the dissertation literature review. *Practical Assessment, Research, and Evaluation*, 14, 2009. Available at: <https://scholarworks.umass.edu/pare/vol14/iss1/13>.
- [Rob11] Colin Robson. *Real World Research*. John Wiley & Sons Ltd, 3rd edition, 2011.
- [Rou20] Margaret Rouse. security information and event management(siem), 02 2020. Available at: <https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM>, Accessed: 20-05-22.
- [Sel19] Caroline Stensland Selte. How moving from traditional signature analysis to automatic anomaly analysis affects user experience and security awareness. Project report in TTM4502, Department of Information Security and Communication Technology, NTNU – Norwegian University of Science and Technology, December 2019.

- [SHF<sup>+</sup>15] Mirjam Seckler, Silvia Heinz, Seamus Forde, Alexandre N. Tuch, and Klaus Opwis. Trust and distrust on the web: User experiences and website characteristics. *Computers in Human Behavior*, 45:39 – 50, 2015. Available at: <http://www.sciencedirect.com/science/article/pii/S0747563214006827>.
- [Slo87] Paul Slovic. Perception of risk. *Science*, 236, April 1987. Available at: [https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/22394/slovic\\_241.pdf?sequence=1](https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/22394/slovic_241.pdf?sequence=1).
- [SP10] R. Sommer and V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy*, pages 305–316, 2010. Available at: <https://ieeexplore.ieee.org/abstract/document/5504793>.
- [Str90] Detmar W. Straub. Effective is security: An empirical study. *Information Systems Research*, 1(3):255–276, 1990. Available at: <https://doi.org/10.1287/isre.1.3.255>.
- [Sym19] Symantec Corporation. 2019 internet security threat report. Technical report, Symantec Corporation, April 2019. Available at: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf>.
- [SZSS16] Nur Farhana Samsudin, Zarul Fitri Zaaba, Manmeet Mahinderjit Singh, and Azman Samsudin. Symbolism in computer security warnings: Signal icons and signal words. *International Journal of Advanced Computer Science and Applications*, 7, 2016. Available at: <https://pdfs.semanticscholar.org/8aaf/c03e35839fa96ab5d151f511ff3f2fb1d31.pdf>.
- [Tjo10] Aksel Tjora. *Kvalitative forskningsmetoder i praksis*. Gyldendal Akademisk, 2010.
- [TJSB07] Miles Tracy, Wayne Jansen, Karen Scarfone, and Jason Butterfield. Guidelines on electronic mail security. <https://csrc.nist.gov/publications/detail/sp/800-45/version-2/final,022007>.
- [TTC<sup>+</sup>19] Michael Theis, Randall Trzeciak, Daniel Costa, Andrew Moore, Sarah Miller, Tracy Cassidy, and William Claycomb. Common sense guide to mitigating insider threats. Technical Report CMU/SEI-2018-TR-010, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 02 2019. Available at: <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540644>.
- [Ver19] Verizon. 2019 data breach investigations report. Technical report, Verizon, 2019. Available at: <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>.
- [WE05] Ye Diana Wang and Henry H. Emurian. An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, 21(1):105 – 125, 2005. Available at: <http://www.sciencedirect.com/science/article/pii/S0747563203001092>.

- [Wel17] Susie Weller. Using internet video calls in qualitative (longitudinal) interviews: some implications for rapport. *International Journal of Social Research Methodology*, 20(6):613–625, 2017. Available at: <https://doi.org/10.1080/13645579.2016.1269505>.
- [Yin09] Robert K. Yin. *Case Study Research Design and Methods*. Sage publications, 5th edition, 2009.



# Appendix

## **Information to interview participants**

This information sheet was given to all employees in the case organization as information about the project and an invitation to participate. It also includes a scheme for consent. The information sheet is based on a template created by NSD. The presented paper is slightly changed to keep the case organization anonymous in this thesis.

Vil du delta i forskningsprosjektet

## ***”Hvordan overgangen fra tradisjonell sikkerhetsanalyse til automatisk avviksanalyse påvirker brukeropplevelse og sikkerhetsbevissthet”***

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke effekten nye sikkerhetsmekanismer for epost har på brukere av epostsystemer. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

### **Formål**

Dette prosjektet gjennomføres ifm en masteroppgave som skrives av en student ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU. Formålet med prosjektet er å undersøke hvordan brukerne av epostsystemer påvirkes av endring i underliggende teknologi som analyserer lenker og vedlegg for å oppdage ondsinnet epost. Vi skal undersøke om bruker blir mer eller mindre sikkerhetsbevisste og hvordan brukeropplevelsen endres. I tillegg vil vi se på om brukerne opplever at personvernet deres er ivaretatt med den nye teknologien.

### **Hvem er ansvarlig for forskningsprosjektet?**

NTNU er ansvarlig for forskningsprosjektet.

### **Hvorfor får du spørsmål om å delta?**

Du får spørsmål om å delta fordi vi i studien skal studere hvordan de nye systemene fungerer i en eksempelorganisasjon, og du er ansatt i denne organisasjonen. Vi ønsker et representativt utvalg av ansatte, med forskjellig bakgrunn.

### **Hva innebærer det for deg å delta?**

Hvis du velger å delta i prosjektet, innebærer det at du deltar på et intervju. Det vil ta cirka 45 minutter, og det vil bli gjort lydopptak av intervjuet. Under intervjuet vil du få spørsmål om ditt forhold til informasjonssikkerhet, spesielt knyttet til epost.

### **Det er frivillig å delta**

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

### **Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger**

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. De som vil ha tilgang til data tilknyttet prosjektet er masterstudenten og noen få ansatte ved NTNU og i din



organisasjon. Dataene vil bli lagret slik at ingen uvedkommende får tilgang til personopplysningene. Du vil ikke kunne gjenkjennes i publikasjonen.

### **Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**

Prosjektet skal etter planen avsluttes 10.06.2020. Ved prosjektslutt vil personopplysninger og lydopptak bli permanent slettet.

### **Dine rettigheter**

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

- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

### **Hva gir oss rett til å behandle personopplysninger om deg?**

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

### **Hvor kan jeg finne ut mer?**

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

- NTNU / Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved masterstudent Caroline Selte
- Maria Bartnes
- Din organisasjon sitt personvernombud: NSD
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 55 58 21 17

Med vennlig hilsen

Maria Bartnes  
(Forsker/veileder)

Caroline Stensland Selte  
(Masterstudent)

---

# Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet "*Hvordan overgangen fra tradisjonell sikkerhetsanalyse til automatisk avviksanalyse påvirker brukeropplevelse og sikkerhetsbevissthet*", og har fått anledning til å stille spørsmål. Jeg samtykker til:

- Å delta i et intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. 10.06.20

---

(Signert av prosjektdeltaker, dato)

## Appendix

# Information to all employees in the case organization

This information sheet was given to all employees in the case organization as information about the project, especially regarding the collection of data from the inbox with reported emails. The information sheet is based on a template created by NSD. The presented paper is slightly changed to keep the case organization anonymous in this thesis.

Informasjon om deltakelse i forskningsprosjektet

## ***”Hvordan overgangen fra tradisjonell sikkerhetsanalyse til automatisk avviksanalyse påvirker brukeropplevelse og sikkerhetsbevissthet”***

Dette er informasjon til deg om et forskningsprosjekt hvor formålet er å undersøke effekten nye sikkerhetsmekanismer for epost har på brukere av epostsystemer. I dette skrevet gir vi deg informasjon om målene for prosjektet og hvordan dette påvirker deg.

### **Formål**

Dette prosjektet gjennomføres ifm en masteroppgave som skrives av en student ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU. Formålet med prosjektet er å undersøke hvordan brukerne av epostsystemer påvirkes av endring i underliggende teknologi som analyserer lenker og vedlegg for å oppdage ondsinnet epost. Vi skal undersøke om bruker blir mer eller mindre sikkerhetsbevisste og hvordan brukeropplevelsen endres. I tillegg vil vi se på om brukerne opplever at personvernet deres er ivaretatt med den nye teknologien.

### **Hvem er ansvarlig for forskningsprosjektet?**

NTNU er ansvarlig for forskningsprosjektet.

### **Hvorfor får du dette informasjonsskrivet?**

Du får dette informasjonsskrivet fordi du har rapportert inn e-post. Disse e-postene inneholder personopplysninger om deg i form av e-postadresse og navn, og vil bli brukt som informasjonskilde i masteroppgaven.

### **Hva innebærer dette for deg?**

Det innebærer at vi kan bruke e-post du har rapportert som informasjonskilde. Hvis du ikke ønsker at vi behandler dine personopplysninger, kan du ta kontakt og alle e-postene du har rapportert inn vil bli utelatt fra undersøkelsen. Dette vil ikke ha noen negative konsekvenser for deg.

### **Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger**

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrevet. Vi behandler opplysningene konfidensielt og i samsvar med personopplysningsloven. Dataene vil bli lagret slik at ingen uvedkommende får tilgang til personopplysningene, og du vil ikke kunne bli gjenkjent i publikasjonen.

### **Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**

Prosjektet skal etter planen avsluttes 10.06.2020. Ved prosjektslutt vil ikke studenten ha tilgang til innboksen lenger.

## **Dine rettigheter**

Så lenge du kan identifiseres i datamaterialet som studenten har tilgang til, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

## **Hva gir oss rett til å behandle personopplysninger om deg?**

Vi behandler opplysninger om deg basert på allmenn interesse fordi behandling av opplysningene er nødvendig for å oppnå prosjektets formål og innhenting av samtykke er umulig/uhensiktsmessig.

På oppdrag fra NTNU har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

## **Hvor kan jeg finne ut mer?**

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

- NTNU / Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved masterstudent Caroline Selte
- Maria Bartnes
- Din organisasjon sitt personvernombud: NSD

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost ([personverntjenester@nsd.no](mailto:personverntjenester@nsd.no)) eller på telefon: 55 58 21 17.

Med vennlig hilsen

*Maria Bartnes*  
(Forsker/veileder)

*Caroline Stensland Selte*  
(Masterstudent)



# Appendix **C**

## **Interview guide**

This interview guide was originally written in Norwegian as the interviews were carried out in Norwegian. Here follows a translated version.

Introduction[ca 7 min]

Presentation of the interviewer and some information about the project.

1. Is it clear for you or do you have any questions before we start?

### **Warm-up questions**

1. Can you tell me just briefly what your work is?
2. Have you ever experienced that someone has succeeded in attacking you through email?

Main part[ca 33 min]

### **Security awareness and risk perception**

1. Which threats do you think your organization is exposed to through the use of email?
  - a. Which consequences can these threats have?
  - b. How worried are you about these threats?
  - c. What do you do to avoid these threats?
2. What do you look for in an email to reveal malicious intentions?
  - a. How do you assess the links and attachments?
3. What do you do if you receive a suspicious email?
4. What do you think your organization is doing to handle malicious email?
5. How do you think your actions with email can affect your organization's security?

### **User experience**

1. Have you noticed any changes in the email system you use the last six months?
  - a. If yes: which changes?
  - b. If no: have you seen anything new with the presentation of links?
  - c. Which advantages do you see with the new presentation of links?
  - d. Which disadvantages do you see with the new presentation of links?
  - e. Do you do any different assessments when receiving email now than?
    - i. Which and why?
  - f. Do you experience any difference in the filtering of spam, in the way that you receive more spam in your inbox or that more genuine email is sent to the spam folder?
2. Do you have any other thoughts about how the system works with the changes?

### **Email analysis:**

Show a set of emails that have been reported as suspicious in the organization, and ask the participant how they would analyze each email if they received it in their inbox. Focus on the analysis of links. Emails attached at the end of this interview guide.



**Follow-up on user experience**

1. Do you have any suggestions to how this email system can be developed to make it even easier for you to assess the email and make more secure choices?

**Privacy and trust:**

1. Do you trust that the email system is helping you in deciding which email is safe and not?
  - a. Why/why not?
  - b. Do you expect that from this kind of system?
2. How do you think the system is able to do the necessary analysis? (If they don't know, explain)
  - a. What do you feel about sharing personal information so that the system can work this way?
3. Do you feel that your privacy is protected through the use of this system?
  - a. If not: Does it affect your experience of using the system?

Ending[ca 5 min]

**Cool-off:**

1. Do you feel that you have the necessary knowledge to evaluate the emails that you receive?
2. Do you remember how you reacted to the constructed phishing email that was sent from the IT department this fall?

**Closure:**

Are there any experiences you have with this that has not been covered in the interview and you want to share?

Thank you for your time.

## Reported emails

### Email 1:

Faktura #10480675

F Feride Emel K. Bærø <feb.nnko@mail.emailsrvr.com>  
ma. 16.04.2018 07:23

#### Ny faktura

Følgende utstillere har sendt en faktura til deg

Utstillere	<b>eFaktura ASP</b>
Logg Inn	<b><u>Se meldingen på webområdet ditt</u></b>
Mottaker	<b>***** AS</b>
Fakturanr	<b>10480675</b>
Fakturadato	<b>04-10-2018</b>
Førfallsdato	<b>05-09-2018</b>
Beløp inkl. skatt (NOK)	<b>12 005 000,00</b>

Den här fakturan levererades av InExchange

yaslipbrasil.com.br/classificados/admin/ /microsoftofficeonline%7C#

### Email 2:

Nytt og Enklere Fakturaprogram.eml ☑ Lagre i OneDrive

L Lett-Faktura <post@lett-faktura.net>  
ti. 25.02.2020 18:19

Fakturering skal være enkelt og raskt.

Lettfaktura revolusjonerer faktureringen – dessuten til en uslæelig lav pris.

Last ned nå og se for deg selv: [www.lett-faktura.net](http://www.lett-faktura.net)

Lurer du på noe – ikke nøl med å kontakte meg på [info@lett-faktura.net](mailto:info@lett-faktura.net)

Ha en flott dag.

Med Vennlig Hilsen

Christian

**LettFaktura**

Pb. 188 3166 Tolvsrød  
Telefon: 31 10 30 00  
Telefaks: 31 10 30 01

NB! Vennligst ikke svar til denne mailadresse siden denne postkassen ikke leses av mennesker. Bruk i stedet kontakt delen på vår hjemmeside.

Vi setter pris på at dere har valgt å være en del av vår malliste. Hvis dere ønsker å legge til en annen emailadresse eller ikke lenger ønsker å være en del av mallisten, vennligst besøk vår hjemmeside, eller:  
Click here to unsubscribe: <http://www.lett-faktura.net/malliste.html>

For oss har «privacy» vært viktig i svært lang tid. Vi har derfor siden lang tid vært tilpasset GDPR.

Vi ønsker ikke heller å holde noen personlig informasjon om dere på vår malliste, slik at den eneste informasjon som vi holder er selve emailadressen som denne mail er sendt til. Der finnes ikke heller noen kobling til navn eller person, uten den eneste informasjonen vi holder utover email adressen, er når dere valgte å være en del av vår malliste.

https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.lett-faktura.net%2F&data=02%7C01%7C...%41...ø%7C9b7b3c8f

### Email 3:

(Viktig): Kortet ditt er blokkert! 20-02-20... Lagre i OneDrive

(Viktig): Kortet ditt er blokkert! 20-02-2020.

Nettbank | SpareBank 1 <kontakt.web@imgpneo.onmicrosoft.com>  
to: 20.02.2020 09:24

Kjære kunde!

For å beskytte mot uautorisert bruk har kortet ditt blitt sperret for ytterligere kjøp med Verified by Visa som en forholdsregel. Hvis du vil fortsette å bruke kortet ditt som normalt, klikker du på lenken nedenfor og følger instruksjonene.

[>>> Logg inn](#)

Denne prosedyren tar bare noen få minutter av tiden din

Takk for din forståelse

<https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.comhouse.biz%2Fcom%2Findex2.php&data=02%7C01%7C...%4C>

### Email 4:

Fibers

Metall Fiber <steelfiber.type1@gmail.com>  
on: 04.03.2020 20:18

Dear Sir or Madam,

I would to introduce our group of companies. We specialize in the manufacturing of:

- Steel Fiber (glued and loose), Steel Microfiber for industrial flooring, tunnels, and concrete.
- Microsynthetic Concrete Fibers and Macrosynthetic Concrete Fibers for shotcrete, for floors or concrete in general
- Glass fiber
- Blowing Glass wool, Blowing mineral wool

Our fibers used in many contries of the European Union, the USA, the Middle East and many other places around the Globe. We can offer of our technology for using a mixture of steel fiber and synthetic fibers in concretes. This technology allows you to improve the quality of concrete and save money. We have technical specialists who can make a calculation.

Our prices are very competitive and we can provide a wide range of fibers in a variety of shapes and sizes

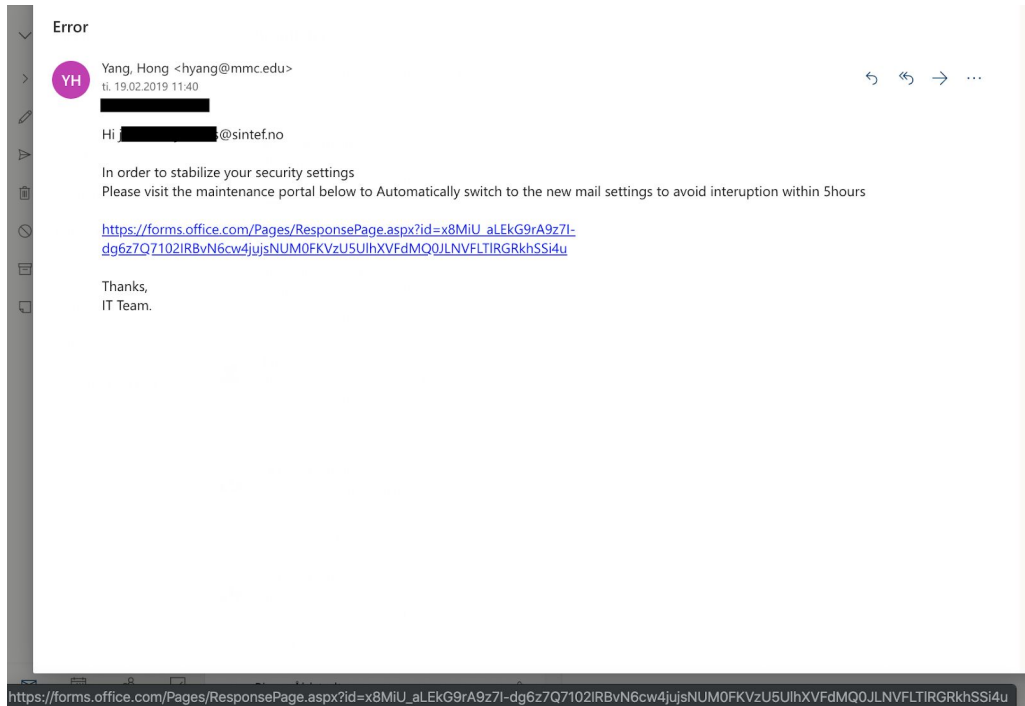
If you interested in our products, more detailed information is available.

Thank you in advance and I look forward to hearing from you soon.

Sincerely,

Slavik Burdeev  
Sales Manager  
CONTINENTAL, Inc  
Phone 3111510  
Fax. 3370855  
conti.ukr@gmail.com  
<https://eur03.safelinks.protection.outlook.com/?url=www.continental.dn.ua&data=02%7C01%7C...%40...%7C5333151e6afb491f6d2d08d7c070da5f%7Ce1f00f89604145b0b309e0210d8b32a%7C1%7C1%7C637189463242011461&data=kiFTY5vgNQJgn%2FP2yQ2h6%2FmrF2rfsQBN7eh9RtOXIMg%3D&reserved=0>

## Email 5:



## Email 6:

### INFO



Helen Jefferson <admin@michaalmount.co.za>

ti. 19.11.2019 13:40

Recipients <admin@michaalmount.co.za> ⌵



Euro-Million Lottery (1).pdf

252 kB

Kindly download and open the attachment for details.

**Email 7:**

**Outstanding INV399650**



IT Service Desk <3302@hanwha.co.kr>

ma. 09.03.2020 10:37

[Redacted] ↕



2 vedlegg (15 kB) Last ned alle Lagre alle i OneDrive – SINTEF

Hello [Redacted]@[Redacted].no,

Due to recent upgrades on our servers You have (1) outstanding invoice


We are sorry for the inconvenient.



Poweredby: Microsoft Corporation.

**Email 8:**

Your Office 365 account is about to be de... [Lagre i OneDrive](#)

Re: Your Office 365 account is about to be deleted

 office-365@security.onmicrosoft.com  
fr. 15.03.2019 20:46

**Your Office 365 Business Essentials Invoice is ready**

[Sign in to the Office 365 Admin center](#) To Pay your Invoice

[View this message in the Office 365 message center](#)

To customize what's included in this email, who gets it, or to unsubscribe, [href=]set your Message center preferences.

[Edit release preferences](#)

Choose the release track for your organization. Use these settings to join First Release if you haven't already.

*Microsoft respects your privacy. To learn more, please read our [Privacy Statement](#).*

*Microsoft Corporation  
One Microsoft Way  
Redmond, WA, USA 98052*

[Unsubscribe](#)

https://kanyreview.cu.ma/blog/s4/index.php?m=... 17.03.2019 [inbox]



# Appendix **D**

## **Research approval from NSD**

The research project was reported to the Norwegian Center of Research Data, and this is their approval of the research.

# NSD NORSK SENTER FOR FORSKNINGSDATA

## NSD sin vurdering

### Prosjekttittel

How moving from traditional signature analysis to automatic anomaly analysis affects user experience and security awareness

### Referansenummer

507981

### Registrert

30.01.2020 av Caroline Stensland Selte

### Behandlingsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet NTNU / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

### Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Maria Bartnes

### Type prosjekt

Studentprosjekt, masterstudium

### Kontaktinformasjon, student

Caroline Stensland Selte

### Prosjektperiode

01.02.2020 - 10.06.2020

### Status

05.03.2020 - Vurdert

## Vurdering (1)

---

### 05.03.2020 - Vurdert

Det er vår vurdering at behandlingen vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet den 05.03.20 med vedlegg, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

### MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde:



[https://nsd.no/personvernombud/meld\\_prosjekt/meld\\_endringer.html](https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html)

Du må vente på svar fra NSD før endringen gjennomføres.

## TYPE OPPLYSNINGER OG VARIGHET

Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 10.06.20.

### LOVLIG GRUNNLAG FOR UTVALG 1

Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

### LOVLIG GRUNNLAG FOR UTVALG 2

Prosjektet vil behandle personopplysninger med grunnlag i en oppgave av allmenn interesse. Det vil kun behandles navn og eventuelt enkelte bakgrunnsopplysninger. Opplysningene vil ikke være sensitive og behandles i en svært kort periode. NSD vurderer derfor at nytten av opplysningen i prosjektet klart overstiger ulempen for de registrerte.

Vår vurdering er at behandlingen oppfylder vilkåret om vitenskapelig forskning, jf. personopplysningsloven § 8, og dermed utfører en oppgave i allmennhetens interesse.

Lovlig grunnlag for behandlingen vil dermed være utførelse av en oppgave i allmennhetens interesse, jf. personvernforordningen art. 6 nr. 1 bokstav e), jf. art. 6 nr. 3 bokstav b), jf. personopplysningsloven § 8.

## PERSONVERNPRINSIPPER

NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen:

- om lovlighet, rettferdighet og åpenhet (art. 5.1 a)
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

### DE REGISTRERTES RETTIGHETER – UTVALG 1

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

### DE REGISTRERTES RETTIGHETER – UTVALG 2

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 14), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), protest (art 21).

NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfylder lovens krav til form og innhold, jf. art. 12.1 og art. art. 14.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

## FØLG DIN INSTITUSJONS RETNINGSLINJER

NSD legger til grunn at behandlingen oppfylder kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32)

OneDrive er databehandler i prosjektet. NSD legger til grunn at behandlingen oppfyller kravene til bruk av databehandler, jf. art 28 og 29.

For å forsikre dere om at kravene oppfylles, må prosjektansvarlig følge interne retningslinjer/rådføre dere med behandlingsansvarlig institusjon.

#### OPPFØLGING AV PROSJEKTET

NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Kontaktperson hos NSD: Silje Fjelberg Opsvik

Tlf. Personverntjenester: 55 58 21 17 (tast 1)

