

Silje Berg and Tilde Thorvik

Social engineering attacks in the light of security economics

Master's thesis in Communication Technology and Digital Security

Supervisor: Maria Bartnes

Co-supervisor: Per Håkon Meland

June 2022

NTNU
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

Silje Berg and Tilde Thorvik

Social engineering attacks in the light of security economics

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Per Håkon Meland
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Title: Social engineering attacks in the light of security economics

Students: Silje Berg & Tilde Thorvik

Problem description:

When discussing the security risks of an IT system, the human users are often declared as the weakest link in the security chain. Social engineering attacks take advantage of this and use various manipulation techniques to fool users into giving away sensitive information or make security mistakes that could be further exploited in a cyber attack.

This study will investigate how common social engineering techniques, such as phishing, spoofing and Business Email Compromise (BEC) can be used to exploit a system, individuals or an organization. We will survey the available literature, and gather information about cases from industry representatives and victims of such attacks. The insights from the data will be synthesized, and evaluated with regards to metrics such as economic loss. Furthermore, we will analyze which economic factors motivate the owners of the system or organization to choose or ignore possible mitigation strategies. This will be generalized to enable a discussion about how the theories of security economics apply to empirical data.

The study requires a multidisciplinary approach, combining information security, behavioral economy and security economic theories to explain the phenomena from the data. Based on our evidence, we hope to create a set of recommendations for practice and further research.

Date approved: 2022-02-28

Supervisor: Maria Bartnes, IIK

Abstract

Security economics is an interdisciplinary field of research that combines economics and security to describe information security shortcomings from an economic point of view. The research field provides a more elaborate understanding of why security breaches still occur despite robust technical measures, and security economics gives an economic framework to analyze cyber security. Social engineering is the art of using manipulation and psychological persuasion to make people compromise information systems.

This thesis looks at social engineering from a security economics context, where the central concepts that are included are *externalities*, *misaligned incentives*, and *asymmetric information*. These concepts are used to discuss phishing, spoofing, and Business Email Compromise (BEC) attacks. The thesis uses a qualitative approach based on in-depth interviews to gather information. Five security experts and four victims of social engineering attacks have participated. The empirical data is used to contribute to the understanding of how to handle social engineering attacks, challenge established ideas like *humans being the weakest link*, provide explanations to why social engineering protection measures fail in practice, and extend the theory of security economics.

The findings uncover new perspectives we argue should be included and discussed further within security economics, mainly the concepts *trust*, *shame*, *transparency* and *culture*. Moreover, based on the empirical data, we provide recommendations to reduce the number of successful social engineering attacks. These recommendations include attitude changes in how we view victims of social engineering and humans in the security chain, policy suggestions, and a new concept we propose, named *Security 2*.

Sammendrag

Sikkerhetsøkonomi er et tverrfaglig forskningsfelt som kombinerer økonomi og sikkerhet for å beskrive mangler ved informasjonssikkerhet fra et økonomisk synspunkt. Forskningsfeltet gir en bedre forståelse av hvorfor sikkerhetsbrudd fortsatt oppstår til tross for robuste tekniske tiltak, og sikkerhetsøkonomi gir et økonomisk rammeverk for å analysere cybersikkerhet. Sosial manipulasjon er kunsten å bruke manipulasjon og psykologisk overtalelse for å få folk til å kompromittere informasjonssystemer.

Denne oppgaven ser på sosial manipulasjon fra en sikkerhetsøkonomisk kontekst, hvor de sikkerhetsøkonomiske konseptene som brukes hovedsakelig er *eksternaliteter*, *feiljusterte insentiver* og *asymmetrisk informasjon*. Disse konseptene brukes til å diskutere angrep som phishing, spoofing og Business Email Compromise (BEC). Denne oppgaven bruker en kvalitativ tilnærming basert på dybdeintervjuer for å innhente informasjon. Fem sikkerhetsekspertene og fire ofre for sosiale manipulasjonsangrep er intervjuet. De innsamlede empiriske dataene brukes til å bidra til forståelsen av hvordan man håndterer sosiale manipulasjonsangrep, utfordre etablerte idéer som *mennesket er det svakeste leddet*, gi forklaringer på hvorfor tiltak mot sosial manipulasjon mislykkes i praksis, og utvide teorien om sikkerhetsøkonomi.

Funnene avdekker nye perspektiver som vi argumenterer for at bør inkluderes i sikkerhetsøkonomi som fagfelt, hovedsakelig begrepene *tillit*, *skam*, *åpenhet* og *kultur*. Basert på empiriske data gir vi dessuten anbefalinger for å redusere antallet vellykkede angrep der sosial manipulasjon brukes. Disse anbefalingene inkluderer blant annet holdningsendringer i hvordan vi ser på ofre for sosial manipulasjon og mennesker i sikkerhetskjeden, forslag til retningslinjer og et nytt konsept som vi foreslår, kalt *Security 2*.

Preface

This master thesis is submitted to the Norwegian University of Science and Technology (NTNU). It is the final submission of our 5-year Master of Science (MSc) in Communication Technology and Digital Security. The research was performed from January to June 2022, and it is a continuation of the pre-project from autumn 2021.

We want to thank our supervisors Per Håkon Meland and Maria Bartnes for their guidance and support. Their enthusiasm, ideas and knowledge have been of great value, both to the resulting thesis, and the process of getting here.

We also want to thank all the interviewees for sharing their time, insight, and knowledge with us. It is greatly appreciated and a significant contribution to this thesis.

Furthermore, we are grateful to our families for cheering on us and supporting us. Your love and encouragement means everything to us.

Finally, a big thanks to our classmates who have made the study experience unforgettable. We value all the discussions and close friendships we have gotten throughout these five years.

Silje Berg and Tilde Thorvik

Trondheim, June 2022

Contents

List of Figures	xi
List of Tables	xiii
1 Introduction	1
1.1 Motivation	1
1.2 Scope and research questions	2
1.3 Contribution	4
1.4 Outline of thesis	4
2 Background	5
2.1 Social engineering	5
2.1.1 Phishing	5
2.1.2 Spoofing	7
2.1.3 Business Email Compromise	8
2.1.4 Reports and examples of social engineering	10
2.2 Behavioral economics	12
2.2.1 Rational choice under certainty and uncertainty	12
2.3 Fundamentals of Security Economics	14
2.3.1 Central concepts of security economics	14
2.3.2 Proposed mitigation measures	16
2.4 Humans as the weakest link	19
2.5 Security culture	20
3 Methodology	21
3.1 Plan	22
3.2 Literature review	22
3.3 Interview process	23
3.3.1 Data management and privacy	23
3.3.2 Interviewees selection	24
3.3.3 Planning the interviews	24
3.3.4 Performing semi-structured interviews	25

3.4	Data analysis	27
3.5	Limitations	29
4	Results	31
4.1	Who are the interviewees?	31
4.1.1	Security Experts	31
4.1.2	Social engineering victims	33
4.2	Results related to existing security economics theories	36
4.2.1	Incentives	36
4.2.2	Externalities	39
4.2.3	Asymmetric information can cause challenges regarding risk quantifying	40
4.3	Interdisciplinary findings	40
4.3.1	Bad luck that a social engineering attack was successful?	41
4.3.2	Usability	42
4.3.3	Shame	43
4.3.4	Challenges with security training	44
4.3.5	Trust	45
4.3.6	Other findings	49
4.4	Humans as the weakest link	50
4.5	Protection against social engineering attacks	52
4.5.1	Security awareness improvements	52
4.5.2	Technical measures	53
4.5.3	Attitude change	54
4.5.4	Building a good security culture	54
4.5.5	Policies	55
4.5.6	Costs related to countermeasures	56
5	Discussion	57
5.1	Research Question 1: Security economics in social engineering attacks	57
5.1.1	Misaligned incentives create a dynamic where issues are not properly dealt with	58
5.1.2	New perspectives regarding externalities	59
5.1.3	Decision making is challenged by asymmetric information	62
5.2	RQ2: Theoretical solutions in reality	62
5.2.1	Trade-offs between different needs	62
5.2.2	Attitudes and behavior	64
5.2.3	"This will not happen to me"	68
5.3	RQ3: Challenging the idea of humans as the weakest link	68
5.4	RQ4: Countermeasures and recommendations against social engineer- ing attacks	70
5.4.1	Policies can enforce or weaken the security of a system	71

5.4.2	Aligning security culture with organizational culture	72
5.4.3	Technical measures	72
5.4.4	Attitude change as a defense mechanism	73
5.4.5	List of recommendations	75
5.5	Threats to validity	76
6	Conclusion and Future work	79
6.1	Future Work	80
	References	83
	Appendices	
A	Information to participating security experts	91
B	Information to participating victims	95
C	Interview guide	99
D	Coding	105
E	Admission to Sikkerhetsfestivalen 2022	107

List of Figures

2.1	Newspaper headlines [29, 26, 30]	6
2.2	Phishing email where the sender claims to be Sparebank 1 [2]	7
2.3	IP address spoofing	8
2.4	Masquerading methods	9
2.5	Factors businesses signify is the cause of security breaches, [46]	11
2.6	The relation between a budget line and our preferred choice	13
2.7	Different actors have contrasting motives when creating statistics	15
3.1	Process overview	21
3.2	Literature review process	22
3.3	Semi-structured interview process, adapted from [75]	26
3.4	Step-wise inductive methodology, adapted from [75]	28
4.1	Erlend Andreas Gjære. The picture is sent and approved by Gjære.	32
4.2	Mia Landsem. The picture is sent and approved by Landsem.	32
4.3	Stig Henning Verpe. The picture is sent and approved by Verpe.	32
4.4	Illustration of Emil Havstad	33
4.5	Illustration of Jonas Dahl	33
4.6	Odd Arne Paulsen. The picture is sent and approved by Paulsen.	33
4.7	Illustration of Peter Lund	34
4.8	Illustration of Carl Jensen	35
4.9	Cecilie Fjellhøy. The picture is approved to use by the licensee.	35
5.1	Trade-off security vs. usability	63
5.2	Negative comments on social media about Victim C's experiences	67
5.3	Positive comments on social media about Victim C's experiences	67
5.4	Cartoon about humans as the weakest link, inspired by [43]	69
5.5	Sharing scams [71]	73
5.6	Illustration about switching perception from humans as the weakest link to humans as a security resource	74
D.1	Overview over codes in the coding tool used on the interview to Security Expert A	106

D.2	Example of how we worked together on coding the data	106
E.1	Introduction of our talk on <i>Sikkerhetsfestivalen 2022</i> [68]	107
E.2	Confirmation of acceptance to <i>Sikkerhetsfestivalen 2022</i>	108

List of Tables

4.1	Statements from interviewees regarding how misaligned incentives between actors can influence the security in a system or between systems	37
4.2	Statements on incentives for focusing on and investing in security	38
4.3	Statements from interviewees regarding externalities	39
4.4	Statements from interviewees regarding (asymmetric) information	40
4.5	Statements from the interviewees about their thoughts whether luck is a reason to a successful social engineering attack	41
4.6	Statements regarding challenges with usability and how this can be a reason to why social engineering attacks are successful	43
4.7	Statements regarding challenges with security training	44
4.8	Statements from interviewees regarding trust	45
4.9	Statements from interviewees regarding transparency of security incidents	46
4.10	Statements from interviewees regarding security culture	48
4.11	Statements on additional findings on why security measures fail in reality	49
4.12	Humans being or not being the weakest link	50
4.13	Statements on security awareness improvements recommendations	52
4.14	Statements on how social engineering attacks can be reduced by technical measures	53
4.15	Statements on how social engineering attacks can be reduced by attitude change	54
4.16	Statements on how social engineering attacks can be reduced by building a good security culture	55
4.17	Statements on how social engineering attacks can be reduced by policy measures	55
4.18	Statements on how costs related to countermeasures against social engineering attacks	56

Chapter 1

Introduction

This chapter provides an overview of the thesis. Section 1.1 presents the motivation for the topic of the thesis, while Section 1.2 displays the scope and research questions. Section 1.3 explains our contribution.

1.1 Motivation

Social engineering as a term was conceived in the book *An Efficient Remedy for the Distress of Nations* by economist John Gray in 1842 [37] [34], and the term has since then developed with society. Today, social engineering is a concept mainly discussed within information security as a method for compromising information security systems. Attackers can perform these attacks at low costs and risks, while at the same time reaching a large audience.

At the same time, people become increasingly available in the digital sphere, making them continuously more exposed to the danger of digital social engineering attacks. According to Verizon's Data Breach Investigation Report for 2022, 82% of all security breaches include human actions [79]. After the Russian invasion of Ukraine in February 2022, security, and information security, has become of particular interest to organizations and authorities. As stated by researcher Maria Bartnes on Dagsnytt 18 about the increased security threat that the Russian aggression poses, "It is the employees that have access[...]. We know that many cyber attacks begin with exploiting the human that has access" [76]. This, combined with the high level of human involvement in security breaches, indicates that understanding the human elements of information security is highly important to protect individuals, businesses, and public institutions.

Attackers that use social engineering techniques rely on the idea that "humans are the weakest link in the information security chain" to reach their goals. The famous cryptographer Bruce Schneier expressed this thought in 2000 by stating that *«Only amateurs attack machines, professionals target people. And any solutions*

will have to target the people problem, not the math problem» [65]. This statement articulates the importance of understanding social engineering attacks and the amount of damage they can cause. Social engineering attacks are particularly important to acknowledge because they are often used as gateway attacks for other more sophisticated attacks [82]. Thus, there is a need to understand social engineering attacks better, and understand why these attacks continue to succeed even though they have been discussed for a long time. The field *security economics* can contribute to the understanding of social engineering attacks through new perspectives, an approach suggested by contributors within the field of security [28].

Security economics is an interdisciplinary research field that combines security and economics, allowing researchers to describe information security shortcomings from an economic perspective, which has led to a better understanding of why security breaches still occur despite robust technical measures. Progressively, security economics includes the use of behavioral economics as well, thus psychology is combined with economics and cyber security. Because social engineering relies on using psychological tricks on the victim, it seems fruitful to look into how behavioral economics interwoven with security economics apply to social engineering. However, little has been done to combine the security economics research field with the known challenges related to social engineering until now. To the best of our ability, we have tried to track down research that uses empirical data from social engineering attacks to enhance insight into security economics, without many findings. Washo concludes in his article *An interdisciplinary view of social engineering: A call to action for research* [80] that “Social engineering research lacks a framework within which to view the topic and to apply findings in real-world organizational settings” [80]. We believe that seeing social engineering in the context of security economics can provide useful insight to social engineering. Therefore, this thesis seeks to map out how the existing theories of security economics can be used to shed light on issues with social engineering.

1.2 Scope and research questions

Security economics is a growing field of research, and today there are many concepts from economics that have been included in security economics, such as security econometrics, economics of cybercrime and econometrics of wickedness [53]. To limit this thesis’ scope, we have chosen to focus on some of the most fundamental principles in security economics. These principles are misaligned incentives, externalities, and asymmetric information, which are explained in Section 2.3.1. When the problem description was written, a part of the scope centered around covering economic metrics and known concepts from economics and applying these to social engineering cases. Since then, the scope has adjusted as we learned more, and gained insight through the interviews. Therefore, the focus on economic loss and economic factors

that motivate whether to choose or ignore possible mitigation strategies has decreased. Instead, more focus have been given to themes of human behavior that were uncovered in the interviews, but that have not been included in the literature we have reviewed. We chose to do this because our understanding is that these new topics provide valuable perspectives to security economics as a research field, and contributes in a new way compared to previously written papers that focus more on economic metrics.

Furthermore, we have mainly interviewed representatives from organizations, except for one private individual, Cecilie Fjellhøy, who is known for her participation in the Netflix true crime documentary *The Tinder Swindler* [57]. We saw this as a chance to gain insight from an individual involved in a highly topical case, and therefore we chose to include her in our interviews. The interviewees are presented in Section 4.1. Moreover, all the interviewees represent Nordic organizations, and all victims are Norwegian.

In this thesis we look further into the social engineering attacks *phishing*, *spoofing* and *BEC* and explore such attacks in the light of security economics. We use empirical data to try to give explanations on why social engineering countermeasures fail in practice, try to challenge the idea that "humans are the weakest link" and recommend countermeasures to social engineering attacks. We aim to answer the following Research Questions (RQ):

RQ1: *How can security economics contribute to the understanding of why phishing, spoofing and BEC attacks are successful?*

RQ2: *Why do theoretical solutions to social engineering issues not always work out as expected in reality?*

RQ3: *How can we challenge the general idea that humans are the weakest link within information security?*

RQ4: *Which measures reduce the success rate of social engineering attacks according to our empirical findings?*

To answer these questions this study *synthesizes literature regarding security economics and social engineering attacks* and *connects literature with real-life cases*. When synthesizing literature, we explore existing theories about social engineering attacks and security economics as well as explore countermeasures against social engineering attacks. Moreover, we use existing security economic theories to explain why security countermeasures fail and succeed, along with discussing which measures can be utilized to improve the security of a system. In order to connect literature with real life cases we provide examples of successful social engineering attacks, and explain how these can be understood through security economics perspectives.

Furthermore, we interview organizations and individuals who have been subjected to social engineering attacks and interview industry professionals about trends and experiences. We explore if the results found match the existing theory from the security economics research field. Finally, we provide recommendations on mitigation measures based on empirical findings on how the success rate of social engineering attacks can be reduced.

1.3 Contribution

This thesis explores social engineering attacks in the context of security economics. There is not much research, if any, that has been written previously on social engineering in this context. This thesis contributes to practice on how to handle social engineering attacks and to theory by extending the security economics research field. We also look at how the theory of security economics and social engineering corresponds to real-life experiences. Furthermore, we provide affirmation, as well as challenging statements and reigning beliefs within this topic. Moreover, we introduce known concepts within social engineering that we believe should be included in the security economics research field and be researched further in this context. We also present a list of recommendations for social engineering attacks. This list contains known recommendations that the interviewees have endorsed, along with new recommendations we introduce based on empirical data and literature.

1.4 Outline of thesis

The following parts of the thesis are structured as presented here:

Chapter 2 - Background includes an overview of the existing literature within the field of research, including insights in some social engineering attacks, the fundamentals of security economics.

Chapter 3 - Methodology explains the methodology of the project, including limitations.

Chapter 4 - Results presents the findings from the performed interviews.

Chapter 5 - Discussion contextualizes the findings with the existing literature, and discusses how the findings can shed light on the research questions in the thesis.

Chapter 6 - Conclusion and Future Work concludes the thesis and presents suggestions for future work within the topic at hand.

Chapter 2

Background

This chapter presents background information relevant to this thesis. The chapter is divided into five main sections. Section 2.1 presents information about social engineering, mainly phishing, spoofing, and Business Email Compromise (BEC). Section 2.2 presents theory regarding behavioral economics. In section 2.3 information concerning security economics is shown, looking into some of the central concepts in the research field, proposed mitigation measures, as well as behavioral security economics. In Section 2.4 information about humans as the weakest link is presented and Section 2.5 presents some literature on security culture.

2.1 Social engineering

There are many definitions of social engineering. This thesis defines social engineering as the art of using manipulation and psychological persuasion to make people compromise information systems [48]. Social engineering attacks rely on victims trusting the attacker [82], in order to gain confidential information and access to systems, or perform malicious acts. The increasing amount of incidents and the combination of technical and psychological tools utilized by attackers have made social engineering attacks the most significant threat to the information security field today [4]. Furthermore, over 82% of issues regarding cyber security originate from "human error" [79], hence social engineering techniques are likely involved in most cyber attacks.

There are many techniques within social engineering. This thesis focuses on three of them, phishing, spoofing and Business Email Compromise (BEC), which will be elaborated in Section 2.1.1 to 2.1.3.

2.1.1 Phishing

Phishing is a social engineering technique where the goal for the most part is to retrieve sensitive information from the audience [48], like passwords or credit card

DNB utsatt for massive phishing-angrep

Antallet phishingforsøk har økt enormt denne høsten, opplyser DNB.

Vipps advarer om phishing-angrep:

- Ikke klikk på lenken!

Kriminelle utnytter endringene som i disse dager skjer BankID, melder Vipps.

Nytt phishing-angrep ved offentlig petroleumsinstitusjon

Petroleumstilsynet har blitt utsatt for et phishing-angrep. Det er det andre dataangrepet på en offentlig petroleumsinstitusjon på under ett år.

Figure 2.1: Newspaper headlines [29, 26, 30]

information [82]. The attacker primarily uses email in order to reach a large number of potential victims, both organizations and individuals. Attackers depend on persuasion techniques that make the attacker seem trustworthy, likable and have a sense of authority [32, 44]. Phishing is the most common and widespread form of social engineering [78]. However, the Verizon 2022 Data Breach Investigation Report (DBIR) states that only 2.9% of employees click on phishing emails, but because the scope is so big, they assume that out of their data breach data alone, 33.473.532 accounts were phished [79]. Consequently, phishing scams are common to experience, and the scams often receive a lot of attention in the media, as Figure 2.1 indicates, showing headlines that appeared in Norwegian newspapers in 2020 and 2021.

The Norwegian bank *SpareBank 1* described on their websites in 2021 [2] how "real-time" phishing attacks targets the bank's customers on email and tries to trick them into revealing sensitive information, often by telling the customers that their

bank cards are blocked or that they need to verify information such as passwords or card number. If the customers reveal this, the attacker can gain control of the card. The email is designed to look like it is coming from the bank, as showed in Figure 2.2, with an email address that looks like the bank's email address, exploiting the fact that customers trust a known source [2].

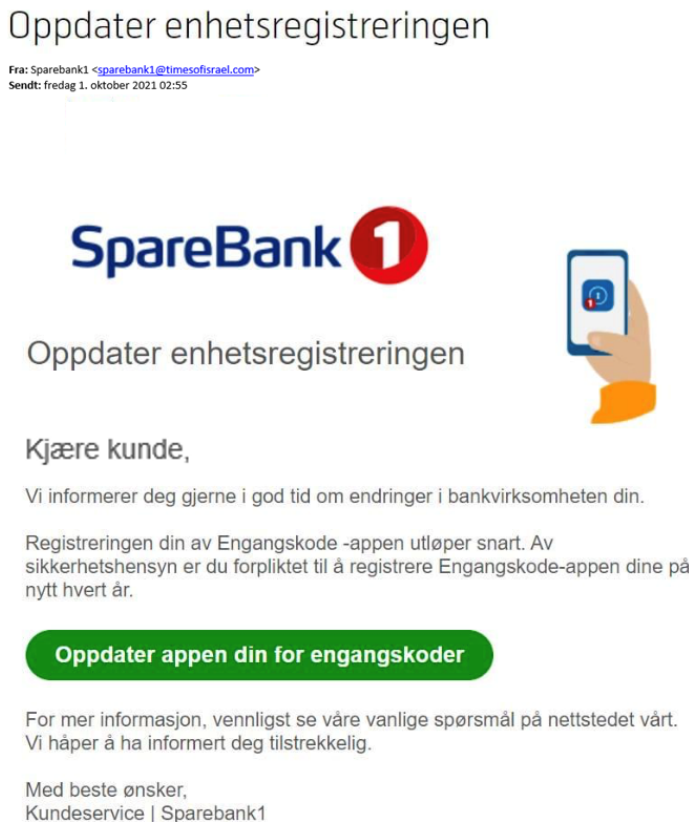


Figure 2.2: Phishing email where the sender claims to be Sparebank 1 [2]

2.1.2 Spoofing

A variation of a phishing attacks is spoofing. Spoofing is a social engineering technique, which targets both individuals and organizations, where the attacker communicates with a victim by impersonating a known and trusted source, and hides where the communication actually originates [44]. By doing so the attacker wants to gain an illegitimate advantage. Attackers can for instance spoof IP addresses to make it look like the IP address is safe and coming from a known source, as illustrated in Figure 2.3, and spoof telephone numbers so it looks like someone is calling from a different

country than what they are [72]. A successful attack is achieved when the messages delivered to the victim seem sufficiently convincing and credible, making the victim perform some action they believe the trusted source asks them to do [44].

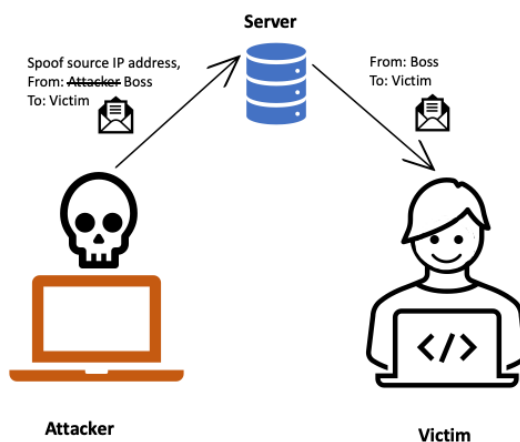


Figure 2.3: IP address spoofing

A recent example of a spoofing attack is when a fraudster called a victim, stating that the call came from the customer service of the victim's bank, and that the call was triggered by what the "bank employee" thought was an attempt of fraud directed at the victim [16]. Through sharing knowledge about the victim's bank details the adversary gained the victim's trust, and gave the victim instructions to "stop" the ongoing fraud, which in reality were instructions to perform an actual fraud towards the victim. By making themselves appear as an actual bank employee the attacker nearly made the victim empty their account [16]. Luckily the victim became suspicious of the credibility of the caller and was able to see through the bluff in this case. This kind of attack largely relies on exploiting the trust of the victims, combined with a sufficient technique for masquerading as another actor.

2.1.3 Business Email Compromise

BEC is a type of phishing attack [6], which relies on email fraud that targets organizations by making it seem as if the sender of the email is legit and a trusted

party [47]. Within the BEC fraud category there is CEO fraud, invoice fraud, blackmailing emails and other types. The goal is to make the victim perform a task for the person the attacker is pretending to be [47]. The attackers try to make the email seem as legit and regular as possible [44]. The FBI's Internet Crime Complaint Center estimates that from 2013-2018 BEC scams accounted for losses over \$1.2 billion [13]. The national center for information security in the municipality sector in Norway (Kommune-CSIRT) reported in their 2021 digital situation picture report that BEC attacks are one of the largest digital threats against organizations [47]. Often legitimate business emails are compromised in these scams and the attacks are normally targeted and rely on the attacker's knowledge of relationships within the organization as well as the organizational structure and procedures [44].

The type of businesses that are targeted are typically those who normally use wire transfers when transferring funds [44], as well as organizations who work with foreign suppliers. The attacker allures to the employees wish to do their job well and the request in the email seems convincing caused by the reasonable context as well as what seems like a trusted party [44].

There are mainly three methods used by attackers to masquerade as a trusted party [44], as visualized in Figure 2.4. The first one is Account Take-Over (ATO), where the attacker gains access over a legitimate email account. Another common method is to spoof the trusted party, and the third method is to create a fake email with a deceptive email domain [44], for example instead of *ole.jensen@hotmail.com*, the attacker makes an email on the form *ole.jensen@hotmail.no*. The goal of this is to execute a form of authority or to gain trust from the victim.

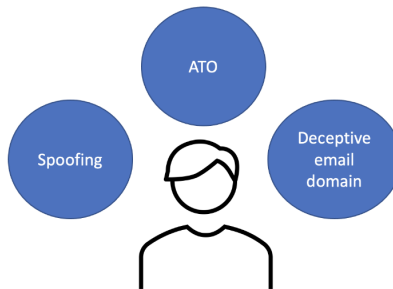


Figure 2.4: Masquerading methods

Ubiquity Networks is a technology company that among other things are improving and maintaining advanced network security. In 2015 the company fell victim to one of the most common BEC scams, showing that even security companies can fall for these

scams [13]. An employee working in the finance department in Ubiquity Networks received an email from what looked like a corporate Ubiquity email address from an executive, informing the employee that the company was performing an acquisition [13]. The email instructed the employee to make payments and said that an attorney would send a new email with instructions of how to conduct the payments. The employee followed the instructions and transferred money. During the following 17 days the employee was sent further instructions from the alleged attorney and made 14 wire transfers that the Principal Financial Officer and Controller of Ubiquity Network authorized with the total amount of \$46.7 million [13]. It turned out the email address from the attorney was a fake email and the recipients of the money was firms that Ubiquity had no business with or knowledge of [13].

2.1.4 Reports and examples of social engineering

The Norwegian bank DNB presents in their Annual Fraud Report 2021 [31] that the number of phishing attacks increased by 512% in 2021 in comparison to 2020. The report also stated that the attacks are more sophisticated than earlier years, which turn even the careful users into victims. Phishing was the fraud with the widest range of victims, where the youngest was under 18 years old and the oldest victim was 93 years, and women and men were equally affected [31]. Moreover, the bank reported that the criminals are more technologically advanced than earlier. DNB reports that the number of customers who have fallen for phishing attacks have increased by 568% from 2020 to 2021, with 3121 DNB customers falling for phishing attacks in 2021 [31].

Mørketallsundersøkelsen [46] is a Norwegian survey that provides an overview of the current situation within IT security in Norwegian private and public organizations. It gathers data about security breaches, cybercrime, and security measures in Norwegian organizations. When asked in *Mørketallsundersøkelsen 2020* [46] whether any alternatives, including *coincident or bad luck, human error, lack of security awareness for employees, existing processes were not followed, insufficient processes* and more were the cause of a security breach in the past year, more than half of the respondents answered that the reason why security breaches occurred was *bad luck or coincidence*. Figure 2.5 showcases the four factors most respondents answered as causes for security breaches.

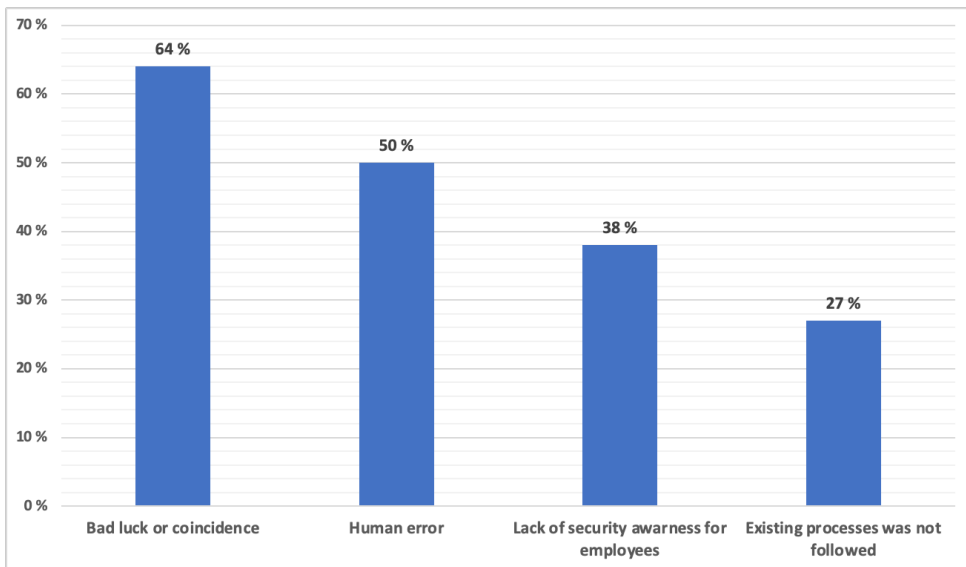


Figure 2.5: Factors businesses signify is the cause of security breaches, [46]

A challenge with cyber-criminality in general, is that the crime often moves across borders and therefore falls between different jurisdictions [17] [69]. This makes it hard to assign a specific authority to process the entire offense. In addition, these cases require resources and might not be prioritized over other criminal investigations. These challenges also apply to phishing, spoofing, and BEC attacks, which can be initiated from anywhere on the globe and reach everywhere, and require cooperation between different stakeholders to investigate. Various victims of these attacks go publicly to the media to broadcast their experiences, and several share their frustration with how the police dealt with their cases [74, 59, 73].

A variety of social engineering approaches exist, some targeting organizations, while others target private individuals. One incident reported by NRK is a crypto scam [74]. A man was tricked into investing close to 200.000 NOK on a fake cryptocurrency exchange platform. Initially, the fraud was started by a woman identifying herself as 'Anna' and asking the man if he was a tour guide. They quickly became friends, and they shared their interest in crypto. Then, Anna introduced him to a crypto platform and encouraged him to invest, but she warned him against investing more than he could afford, earning his trust [74]. Later the man found out it was a fraud, and NRK revealed he was not the only one to be tricked by the scammers behind the fake platform. In fact, this was a significant operation with several fraudsters behind it and several victims involved [74].

2.2 Behavioral economics

Standard economic theories and models are based on several assumptions that simplify the models. However, these assumptions are not necessarily realistic in reality, where it is empirically shown that human behavior deviates from what is expected in the economic models [51]. Behavioral economics applies knowledge from psychology to economics to battle these shortcomings and improve the understanding of why economic models fail to predict a decision-maker's choices, as Mallard describes in the book *Behavioral economics* [51]. This section provides a brief introduction to the research field, focusing on the aspects relevant to security economics, and how these are applied to state-of-the-art security economics research..

2.2.1 Rational choice under certainty and uncertainty

A **rational actor** in economics is someone that makes rational choices to achieve their personal ambitions [11]. Personal ambitions are described using **preferences** the individual has over a set of choices, where some are preferred over others. Rational actors will at all times choose the most preferred alternative. A person's **utility** numerically describes the degree to which they prefer one option over another and can be used to order preferences, where higher utility indicates a more preferred choice [51]. Rational actors will at all times choose the alternative that maximizes their utility when presented with a selection of choices. Utility is helpful within economics because it can explain people's choices not only based on what objectively has the highest value, here personal preferences are also taken into account [11].

Rational consumers will maximize their utility given their budget. Figure 2.6 illustrates a person's possible combinations of two goods, X and Y, along the axes. The curves are *indifference curves*, and the decision-maker receives the same amount of utility at all points on one of these curves. Because decision-makers have limited budgets, illustrated by the *budget line*, the optimal combination of goods X and Y is where the indifference curve meets the budget line, marked in red.

Within security, this means to invest resources in security measures, for example, security awareness training (X) and cyber insurance (Y), that provide the highest level of security given the budget [66]. This model also applies to rational attackers, who likewise have budget constraints and need to identify the optimal combination of various attack techniques. According to the state-of-the-art report about security economics written by the EU project IPACSO in 2016 [45], many of the cyber-security analyses focus on these rational actors on both the defense- and attack side and the cost-benefit trade-offs these actors face.

Whenever elements of choice are uncertain, *probability estimates* are a part of evaluating which option an individual prefers [11]. However, humans tend to either

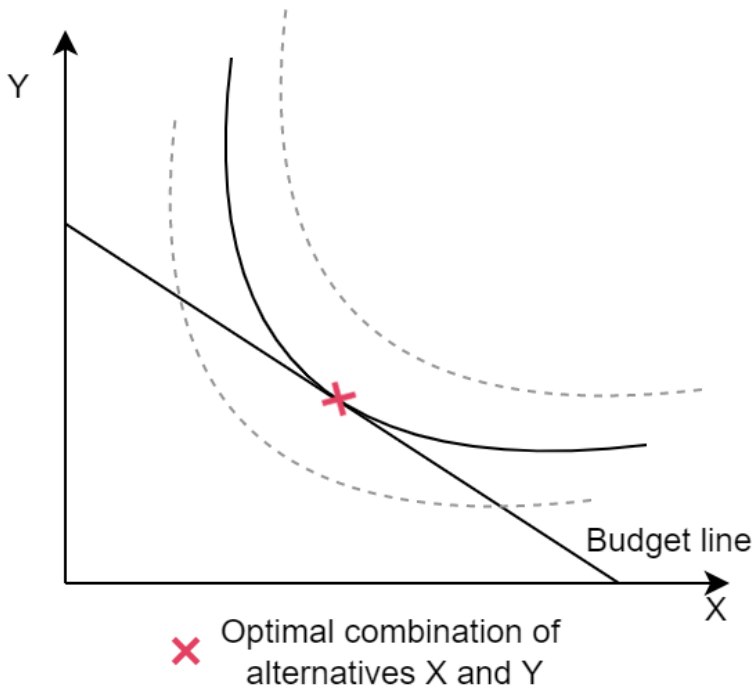


Figure 2.6: The relation between a budget line and our preferred choice

overestimate or underestimate probabilities [66]. Behavioral economics explains this through biases and heuristics, which are cognitive shortcuts a person makes when faced with a decision. One such heuristic is the **availability heuristic**, where a person assigns probabilities that coincide with how easily a corresponding event comes to mind, which is highly individual. This is something decision-makers within security should be aware of because these biases can lead to less efficient security investments [66]. An example Baddeley [12] presented is that people might deem a security issue to be unproblematic because they have not experienced recent events where it arose. Then, the issue does not come easily to mind, and the probability of it occurring is evaluated as lower than it is, and creating countermeasures to protect against the issue is neglected [12].

A bias related to rational choice is the Status Quo Bias. This bias refers to the habit people have of preferring the current state of things above other options [51]. This can be seen when people tend to stick with the default settings that software companies suggests, instead of changing the settings to best fit their needs [67]. This can be exploited to improve security by implementing default settings that favor robust security behavior [12].

2.3 Fundamentals of Security Economics

Security economics involves concepts from economics in the analysis of cyber security. This includes looking at actors in the system and their choices using the same frameworks as in economics, but understanding the choices that specifically affect security [45].

This research field is mainly attributed to Ross Anderson and his work in the early 2000s with connecting economics and cyber security, starting with his article *Why Information Security is Hard - An Economic Perspective* [8]. This article argues that in addition to the technical focus, the use of economic perspectives such as misaligned incentives, asymmetric information, and externalities can explain mechanisms and failings within cyber security.

2.3.1 Central concepts of security economics

Misaligned incentives centers around the challenges that arise when the ones who suffer from a security attack are not the actors who can prevent the attack, and the ones who *can* prevent the attack do not bear the full consequences of the attack, hence they have no incentives to prevent it [9]. Legal theorists recommend making the actor best suited to reduce risk liable for actually reducing the risk [9]. However, in the online world, the responsibility for reducing risk is often misplaced. The actor that can spend resources on security measures may not be emotionally or financially affected by the attack and therefore, the utility of such an investment will be too low to justify the investment [9]. One example Anderson presents is that an individual is willing to pay large sums for anti-virus software to protect themselves, but is unwilling to spend a single dollar on anti-virus software that protects other actors. This scenario is called a moral hazard, meaning it is profitable to be selfish [9].

Another display of this problem regards misplaced liability between banks and customers. Either the customer has to prove that they tell the truth when they claim that they have been scammed, or the bank has to prove that the customer is lying to avoid covering the lost money [8]. Anderson [8] explains that in countries where this responsibility is placed on the banks, the banks impose more robust security measures to stop lying customers, which leads to fewer fraud cases. The banks have the opportunity to protect their systems, and when they have economic incentives to protect themselves, fewer problems arise, Anderson claims [8].

Another concept that is used within the field of economics is *asymmetric information* [9] [8]. This concept concerns the fact that different parties or sides have access to different information in a market, and often that one party has access to *more* information than the other. The fundamental example of these markets is the *Market for lemons*, as described by Akerlof in 1970 [5]. The market he depicted

consists of good quality cars (plums) and bad quality cars (lemons), that should be priced according to their quality, for example \$2000 for plums and \$1000 for lemons. Akerlof showed that when sellers are aware of the quality of a car, but the buyers are uninformed, all cars will be sold at the price of a low-quality car. Because the sellers of high-quality cars are aware that their car is worth \$2000, they want to sell at this price, but when the buyers are unable to know if a car listed at \$2000 is worth \$1000 or \$2000, they are unwilling to pay \$2000. Therefore, no sellers of high-quality cars will be able to get the amount of money they want for their cars, and refrain from putting their cars on the market. Hence, only low-quality cars will be available in the market. This applies to products and services within information security, where the consumers struggle with distinguishing lemons and plums, and as a consequence, the low-quality security products will win most of the market, much to the frustration of the information security community [9] [8].

One example of information asymmetry in information security is that there is a highly limited amount of hard statistics on security attacks and breaches [45]. Furthermore, the actors that create these reports, be it insurance companies or businesses, have different motivations when creating statistics, as illustrated in Figure 2.7. Without the ability to know how extensive the threat of cyber security attacks is, it is difficult to prioritize investments in security [56]. Particularly small and medium sized organizations are inadequately aware of cyber risks and do not invest enough in information security measures [28].

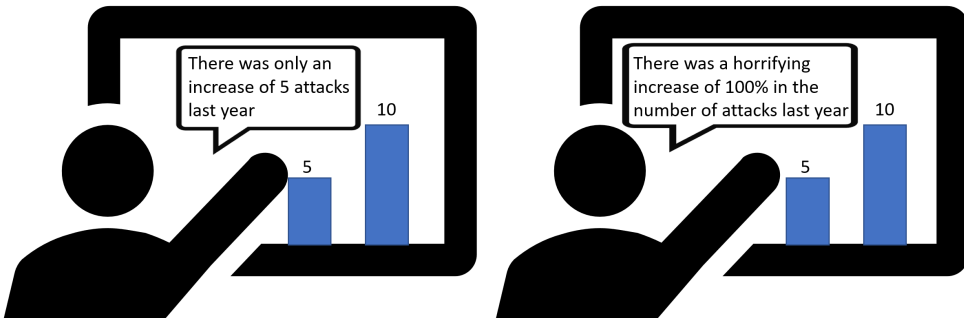


Figure 2.7: Different actors have contrasting motives when creating statistics

Externalities is the costs or the benefits induced on other actors as a result of someone's actions [60]. The most prevalent type of externalities is *network externalities*, where the utility of a network increases for every user when a new user joins the network [8]. In the establishment phase of a product or a company that enters a digital market, it is vital to reach a critical mass of users to win enough of

the market to survive. Therefore, it can be rational not to prioritize a lot of resources on security measures, as these investments may go at the expense of others that are needed to get enough users [8].

Within cyber security, externalities appear when for example someone connects an insecure machine to the Internet. This makes the Internet less secure, while the actor connecting the insecure device is not facing any particular consequence for their actions [10]. Also, many digital platforms rely on complementary actors in order to gain users. More complementary products and services lead to more users joining, and the platform’s value increases. To get enough complementary products in the network, platforms benefit from lowering the requirements for security from the complementary products, thus the security of the platform becomes lower. So, again, it is rational for the actor, in this case, a platform, to choose the sub-optimal security alternative. According to Herley [39], it is rational for consumers not to take security advice if the advice causes a poor cost-benefit trade-off.

Furthermore, if everyone else acts securely, the risk an individual faces if they display less secure behavior themselves is low. This is because security can be seen as a public good that everyone has access to. Therefore, the security of a network is prone to the free-rider problem, where an actor is able to benefit from the actions of others without facing the costs of doing these actions themselves [12].

2.3.2 Proposed mitigation measures

This section provides an overview of the central mitigation measures against cyber attacks that researchers have proposed using the perspectives of security economics. These mitigation measures are primarily based on analysis of why security measures fail from an economic perspective, where the concepts from Section 2.3.1 are relevant tools.

Policies

Security economics researcher Tyler Moore proposed some tangible solutions to mitigate the security risks related to misaligned incentives, externalities, and asymmetric information in a 2010 paper [55]. He suggested a more substantial use of *policy* to align regulations and liability, identify the parties who have the opportunity to solve problems and assign responsibilities accordingly. There are several ways to implement such policies, where some approaches target policy alterations before an attack (*ex ante*) to prevent security incidents. Others focus on changing the policies on what is to happen after a security incident (*ex post*), hoping to create sufficiently severe consequences, making the relevant actors motivated to take action to prevent the attack.

Moore argues that compliance-based security measures are prone to fail and thus not an optimal approach even though they are common in the IT industry [55]. Instead, given an example concerning Internet Service Providers (ISPs), ISPs should be assigned more responsibility for dealing with insecure entities. There should also be mandatory disclosure of security incidents to improve knowledge and make informed choices [55].

Furthermore, even if the security of a system could be bulletproof, this might not be preferred [55]. It is possible to avoid online banking fraud altogether by imposing a policy of not using online banking solutions and use offline alternatives instead. When looking at society as a whole however, this would make the population worse off because offline banking is more costly in terms of time and resources for each individual than the cost of online banking fraud. Thus, there is a trade-off between security and efficiency, where some amount of insecurity needs to be accepted. In this trade-off, misaligned incentives can cause the decision-making actor to choose an alternative that is less optimal for society, because the sub-optimal alternative is the most beneficial for the actor. This means that even policy choices are affected by misaligned incentives, which makes creating good policies even more challenging [55].

Stricter law enforcement will increase the chances of being caught, according to Bauer and van Eeten [14]. Higher penalties for cyber-crime increase the cost of criminal activity, thus the benefit of cyber-crime decreases, and fewer individuals will engage in cyber-criminal activities [14]. Baddeley [12], on the other hand, argues that fines and penalties are not effective enough at reducing the number of phishing attacks and online fraud, because the chance of being caught is low due to the limited capacity of crime-fighting authorities. Therefore, Baddeley claims that an efficient measure against cyber-security attacks is to encourage people to take more responsibility themselves to stop the attacks and protect their privacy.

Information Security Awareness

According to Pyzik [64], increased Information Security Awareness (ISA) is one of the best mitigation measures against a social engineering attack. The main goal is to raise awareness around security threats and risks, thus influencing the users' behavior to act more cautiously in order to protect data and networks. Examples of the training can be reminded of reading URLs properly, before clicking on them, reading email addresses, and checking the email domain.

However, multiple studies conclude that "traditional security awareness training" that focuses on what employees should and should not do as well as awareness of risks and threats is ineffective in regards to changing employees' behavior [40]. Studies conclude that employees are aware of what they should and should not do, but that their behavior does not reflect their knowledge [40]. Some of the reasons behind this

pointed out in literature is that some of the security behavior is not possible for the employees to perform, or the behavior would lead to a considerable decrease in productivity, making the employees feel obligated to "cut corners" [40]. Hence, it is important for organizations to understand compliance behavior when they want the employees to help strengthen the information security within the organization and follow the advice in security awareness training [18]. Seeing when employees comply with the organization's security policies and regulations they can serve as an asset in regard to information security [18].

Cyber insurance

Cyber insurance is another measure for managing information security risks [54]. Böhme and Schwartz define cyber insurance as *"the transfer of financial risk associated with network and computer incidents to a third party"* [20]. The insured party pays an annual fee to the insurance company in order to be covered if an unforeseen security incident is affecting the insured party [53]. The insurance company sells insurance policies based on past losses and future predictions [53]. Moore [54] states that such insurance could create incentives for both organizations and individuals to take extra precautions. Moreover, actors who take fewer risks could be rewarded by the insurance company by getting a lower price for instance, which would create incentives for the insurance company to collect data on security incidents, hence also helping with the information asymmetry problem that exists in the market [54]. Cyber insurance is however a relatively new concept and it struggles to become prominent in the market, even though there is strong market potential [83]. However, one challenge with cyber insurance estimates is that several of the assessments are based on non-scientific studies performed by actors who have economic motives for overestimating the costs, since a higher estimated cost of failure allows for higher insurance fees [28].

Information sharing

Ineffective investments in security are costly, and the overall security is enhanced when resources are used optimally. As described in Section 2.2.1 a challenge is that decision-makers wrongfully assign probabilities to various risks. One measure to reduce the risk of biased probability estimations is to share information about incidents [66]. This can scale down a person's subjective perspective on probabilities, which leads to a more objective and rational analysis of resource allocation within a security budget, and better utilization of the resources.

Technical measures

The United Kingdom's National Cyber Security Centre (NCSC) [21] recommends a multi-layered approach to phishing defenses. The first "layer" is to make it difficult

for attackers to reach users by implementing a "spam filter" to block incoming phishing emails, implementing anti-spoofing controls so that attackers cannot spoof an email address, as well as considering what information is easily available online regarding the organization. The email protocol used today, Simple Mail Transfer Protocol (SMTP) does not authenticate senders, instead it relies on extensions like *Domain-based Message Authentication, Reporting and Conformance* (DMARC) and *DomainKeys Identified Mail* (DKIM) [42]. The second "layer" is to help the users identify and report suspicious emails. NCSC recommends ISA training as well as creating a culture where employees can seek help and report suspecting emails without being "blamed" for doing mistakes or for instance clicking on a phishing link in an email [21]. Layer three recommends ensuring that privileges are only given to those who need them and those privileges are well protected, for instance with a Two Factor Authentication (2FA), as well as keeping hardware up to date with the recent software updates as well as protecting users from malicious websites with for example a proxy server. The last layer says to respond quickly to incidents [21].

2.4 Humans as the weakest link

Humans are often referred to as the weakest link, both in academic papers as well as the media [7, 49, 3, 22, 36, 38]. The statement is used frequently, but rarely justified [82, 84, 19]. Some justifications used to that humans are the weakest link is that most security incidents start with social engineering attacks [63], which relay on manipulating humans.

Sasse and Adams oppose regarding users as the main problem [3]. They highlight that increased technical measures reduce the overall security because the users lose motivation to comply. Namely, stricter password requirements led 50% of the respondents in a survey to either write down their passwords or chose similar passwords across systems. They argue that this behavior does not occur simply because users are stupid and lazy, but because the workload becomes too big to handle. The users intend to act securely, but when the overhead of secure mechanisms becomes too big they make use of shortcuts, which reduce the overall password security more than with a less rigid policy [3]. The recommended countermeasures to this issue include; helping users to construct memorable passwords that are secure, reducing the number of various passwords the user has to remember, for example using Single Sign-On, ensuring that the users understand why the security measures are necessary, and aligning password policies with the organization as a whole [3]. In the article *From Weakest Link to Security Hero: Transforming Staff Security Behavior* Sasse, Pfleeger and Furnham states that humans can be used as a security resource instead of being regarded as the weakest link [61].

Nepal [58] agrees with Sasse and Adams, stating that it is unfair to call humans

the weakest link in the information security chain. He argues that “Blame is often placed on a victim.” [58], and that this problem usually is inherent in society, hence also affects the information security domain. Nepal also argues that “We often forget that underlying security systems should also bear some responsibilities for introducing bugs and vulnerabilities due to the poor practice of designing and building secure systems” [58], and emphasizes that there is not enough focus on usability.

2.5 Security culture

The article *Defining organisational information security culture - Perspectives from academia and industry* [24] defines “Information security culture is contextualized to the behavior of humans in an organizational context to protect information processed by the organization through compliance with the information security policy and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives” [24].

The article states that over time the security culture becomes a part of the organizational culture as an outcome of the values, beliefs, assumption, knowledge and attitude of the employees [24], as well as the information security culture is directed by the management. da Veiga and Martins [25] agrees that the information security culture evolves as a result of the employees attitude, perception and behavior, and this culture either pose a threat to the organization or contribute to protect it.

Chapter 3

Methodology

The study centers around a literature review of the fields of information security and security economics, followed by empirical studies using interviews. We have used qualitative methods, and we believe interviews in combination with a proper literature review is a good approach to answering our research questions. RQ1 can largely be discussed using existing theory from the fields of economics and information security. RQ2, RQ3 and RQ4 require insight into data from the real world, that can be compared with existing theory, leading to the need for gathering empirical data. According to Beck and Manuel [15], interviews are recommended if the goal is to study trends, detailed human issues, or to discuss in prose instead of numbers. Seeing as RQ2 to RQ4 require insight in human issues and can make use of prose rather than numerical data, it seems fitting to choose interviews for gathering empirical data in this thesis. More specifically we use semi-structured interviews, and the rationale for choosing this method is explained in section 3.3.4.

An overview of the process is visualized in Figure 3.1. As illustrated, the process of writing this thesis was not linear. We moved between different phases but still tried to be done with one phase before starting on another one. The different phases are elaborated on in the following sections.

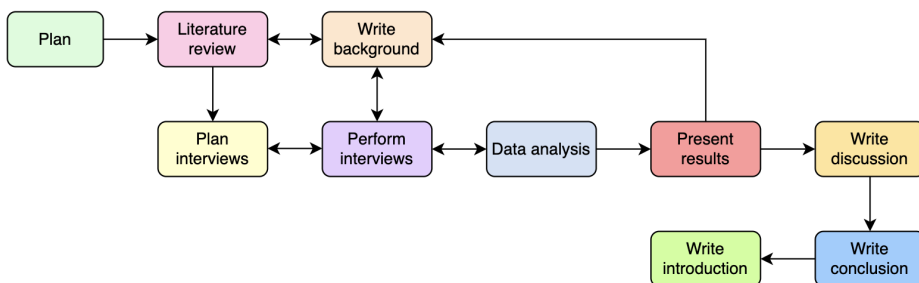


Figure 3.1: Process overview

3.1 Plan

We first started planning how we wanted to work together and which direction to take the thesis in. In this phase, we re-visited the research questions defined in the project assignment and made some alterations. We also used the plan made during the project assignment, specified this even more, and shared our expectations to each other and ourselves. We defined how we should handle conflicts and talked about how we wanted to approach constructive criticism. We also set goals for the end result of the thesis and discussed how we were going to reach these goals while still having a work-life balance.

3.2 Literature review

In order to retrieve satisfactory insight into the fields of research, what has been done previously, and what other scientists within the field deem relevant to investigate in the future, we performed a literature review. This process is illustrated in Figure 3.2 and will be described in the following paragraphs.

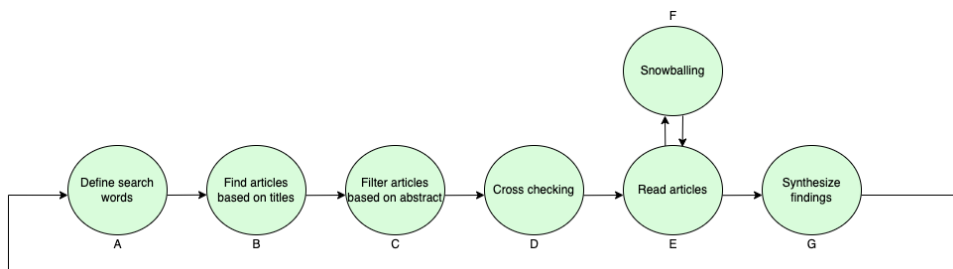


Figure 3.2: Literature review process

In order to find literature the search portals Google, Google Scholar, Oria and ACM Digital Library were used. The following search words as well as combinations of them were used to find a good part of the literature used in this thesis: *social engineering, security economics, information security, behavioral security, behavioral economics, phishing, spoofing, BEC, externalities, asymmetric information, misaligned incentives, social engineering countermeasures, cybersecurity, cybersecurity economics*. In addition to this, Ross Anderson's homepage was used to find further relevant articles. The homepage provides an index of his own articles and they provide valuable insight of the contributions to the security economics research field.

To narrow down the search results from the search engines and Anderson's homepage, the articles and reports with the most relevant titles were chosen. In

addition to filtering on titles we also considered the number of citations of the literature as well as the publishing year to further judge the relevance. After this initial filtering, there was another filtering based on the abstracts of the articles. We then showed the literature we found relevant to the other researcher and then decided together if the article or report seemed relevant to read. This cross-checking ensured that both researchers considered the literature relevant, making the selection process more objective as well as assuring that articles one researcher may have missed, the other researcher could present, making the article eligible for consideration.

As illustrated in Figure 3.2 the next step was reading the article or report. While reading literature, snowballing was used to discover new literature by examining the references and citations used in that article. We read varying publications and shared the key takeaways with each other. Thereafter the findings and information from the literature was synthesized and organized in the thesis to serve as the backbone for relevant literature needed to answer the research questions. Before writing, we discussed the main points to include and made sure we agreed on them so that we could write individually. Following this, we read each other's text and discussed its content. This entire process was repeated multiple times as more literature was needed, as indicated in Figure 3.2, and it was an essential part of writing Chapter 2.

3.3 Interview process

In parallel with the literature review needed to discuss RQ1, the process of gathering data for the thesis was set in motion. Data gathering can be done either quantitatively or qualitatively. Quantitative research is based on gathering numeric data, that can be used to create statistics, say something about the relations between the data, or perform a comparison of aggregated data [23]. Qualitative research focus on gathering insights of the experiences of people, as opposed to quantitative research, focusing more on numbers and statistics [27]. Qualitative research, such as interviews, is not possible to generalize to entire populations, but provide insights into specifics that might be useful either way.

3.3.1 Data management and privacy

After choosing semi-structured qualitative interviews to gather data, the next steps of the interview process consisted of creating an interview guide, reporting the planned interviews to the Norwegian Centre for Research data (NSD), finding interviewees, performing interviews, and processing the interviews afterwards. The NSD documents are attached in Appendix A and B, and the interview guide in Appendix C.

Qualitative interviews can either be done physically, through video call or voice call [81]. The advantage of video call is that it allows for cost-effective conduction of

the interviews, as it saves both money and time on physical travel. When conducting interviews digitally, there is however an increased chance of miscommunication due to the lack of body language and eye contact captured on camera. Most of the interviews were performed on video call using Microsoft Teams because of the physical distance between the researchers and the interviewees as well as the Covid-19 pandemic. These interviews were recorded, with the consent of the interviewees, and stored on NTNU's servers until the transcripts were complete, at which point the recordings were deleted. Two physical interviews were held, where the conversation was recorded using an analog recorder.

3.3.2 Interviewees selection

When choosing interview candidates we mainly used our own network for both of the candidate groups, security experts and victims. We reached out via email to several organizations and individuals, asking if they had expertise on social engineering or if the organization had experienced a social engineering attack and could share the experience with us, anonymously if they wanted. The answers were few, most did not give a respond, and the respondents were even fewer when asked if they had experienced a social engineering attack they could share.

There were a few security experts that could talk to us, but we decided on five individuals that worked in different organizations and could provide different knowledge and perspectives. Three of the security experts are from our own network, while the two others are not, where one answered on an email request and one on a post on an IT security Facebook group.

Because of the difficulty with finding victims, we only have victims from our network or victims who have already talked public about the incident. The four victims have experienced different forms of social engineering, and this is why we chose them for this study, as well as they agreed to be interviewed and share their experience.

3.3.3 Planning the interviews

In order to plan the interviews we worked together to make an interview guide with questions we believed would help answer the research questions. We started with what we were curious about and wanted to find out from both of the interviewees group, security experts and victims, keeping the research questions in mind. Thereafter, we structured the questions under each research question and added questions where it seemed needed. There were some questions we planned to ask everyone, regardless of being an expert or a victim, but then the interview guide was split in two parts; one for the experts and one for the victims, because the questions were quite different for the two groups.

Before conducting the interviews we performed short informal preparatory conversations with two of the potential interviewees, to gather insight of their knowledge and whether or not interviewing them could result in a contribution to the thesis. The main goal with this step was to ensure that we would be properly prepared for the formal interviews as we had never tested out the interview guide before, as well as making sure that it was relevant for the thesis to interview the potential candidates. This also allowed for the interview guide to be updated with questions the interviewees had knowledge about, reformulate unclear questions, as well as finding out if there was a need for more interviewees to cover knowledge gaps. These conversations were then further elaborated on in the formal interviews.

3.3.4 Performing semi-structured interviews

There are several approaches to performing and preparing interviews, mainly structured interviews, semi-structured interviews, and unstructured interviews [81]. The first alternative requires the same questions to be asked to all participants, and no follow-up questions are allowed. This is something we found too restraining for our study, due to the need for different information from different interviewees. We also defined the value of relevant follow-up questions to be major in the interviews, which means that a structured interview is not of particular value to the project. Unstructured interviews are open, more similar to a conversation, without particular guidance regarding the questions to be asked. In order to ensure that the interview touches upon the planned subjects this sort of interview would not be sufficient in order to gather enough empirical data.

A semi-structured interview has an interview guide ensuring that the interview touches upon specific subjects [75]. At the same time it is not as strict as a structured interview, because it allows for follow-up questions when this is deemed valuable [75]. This is seen as a reasonable interview approach for our project because our research questions mandate gathering empirical data, but there might be questions that we as interviewers have not thought of before the interview, but that might emerge when the interviewee talks. There may also be a need to ask the interviewee to elaborate on a theme he touched slightly upon.

As described by Tjora [75], a semi-structured interview consists of three phases, namely warmup questions, reflection questions and round-off questions, as illustrated in Figure 3.3.

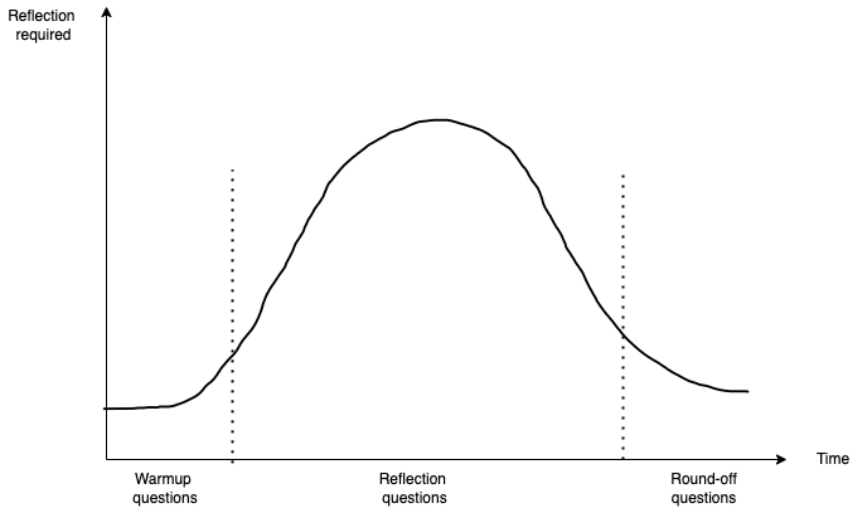


Figure 3.3: Semi-structured interview process, adapted from [75]

During the first phase of the interview, the warmup phase, the questions should be simple and concrete and not require much reflection [75]. The goal is to make the questions seem informal and easy. In this phase we first started off by asking for approval to record the interview as well as introducing ourselves and the study. Then we proceeded to ask if the interviewee could introduce singular background. Afterwards we moved on to the reflection questions, which is the core of the interview [75]. This is the phase where the interview guide was used. The total interviews lasted about an hour to 90 minutes, where this phase normally lasted 45 to 75 minutes. About 9-11 questions were asked from the interview guide during this phase as well as follow up questions where this was needed.

Thereafter, we initiated the round off phase where the intention is to lead the attention of the interviewees away from the higher reflection level and to normalize the conversation [75]. In this phase we asked if the interviewees had any last reflections or any questions regarding the thesis. Afterwards we thanked the interviewees for their time, and explained how the information provided would be used in the thesis. It was explained that we could send them the parts of the thesis where their data was used before the thesis was complete, so they could see if they approved of the way it was written. After each interview we learned more of how well the interview guide worked, and we improved the formulation of some of the questions that were unclear or added some of the follow up questions we asked to be a permanent question in the interview guide.

3.4 Data analysis

The data analysis was performed using triangulation, i.e mixed methods, in order to present the result. One of the methods used was inspired by the step-wise inductive methodology by Aksel Tjora in [75], where some the steps were altered to fit our needs and processes. This methodology is illustrated in Figure 3.4.

In Step One, we created an interview guide, a detailed description of which can be found in Section 3.3.3. In Step Two we conducted the interviews. As we conducted the interviews, we took notes and recorded the conversation, which resulted in "raw" empirical data used for the further analysis of the data. After each interview we went over the interview guide to update it based on the feedback from the interviewees as well as improving some of the formulations of questions that were unclear to the interviewee.

Moving on to Step Three, we transcribed the interview to make working with the empirical data easier. This constituted the foundation for Step Four, where we coded the transcribed interviews. Coding qualitative data is a method of turning the raw data into a story by identifying the most relevant topics and elements by labeling words, paragraphs, and sentences with a word or a phrase that summarizes the content [50]. This was done to get an overview of what the interviewees talked about and what they emphasized when asked about different topics. Before the coding started, we identified the codes we regarded as relevant based on the research questions and the prominent themes uncovered during the transcription phase. The codes *incentives*, *externalities*, *asymmetric information*, *security training*, *bad luck*, *humans as the weakest link*, *technical measures*, *security culture*, *policies* and *security training* were the most central codes we established to cover the topics from the literature review, which formed the basis of the interview guide. During the interviews and transcription phase, the new themes of *usability*, *shame*, *trust* and *attitude change* appeared and were added to the set of codes. During the process, we nuanced the code about humans as the weakest link between *agreeing* and *disagreeing* with the statement. Appendix D displays an excerpt of how the coding looks visually.

We divided the first interviews between us and coded them individually with a coding tool. Then we exchanged interviews and compared to see if our coding was similar. After a few rounds of doing this, we became more harmonized and synchronized in how we coded the text. This served as a base for the results and, together with the background material, constituted the core elements for the discussion.

Then we reviewed the interviews for quotes that captured vital points from each interviewee, so these could be used in tables sorted on different codes in Section 4. We also categorized phrases that were unsuitable as quotes but still captured what

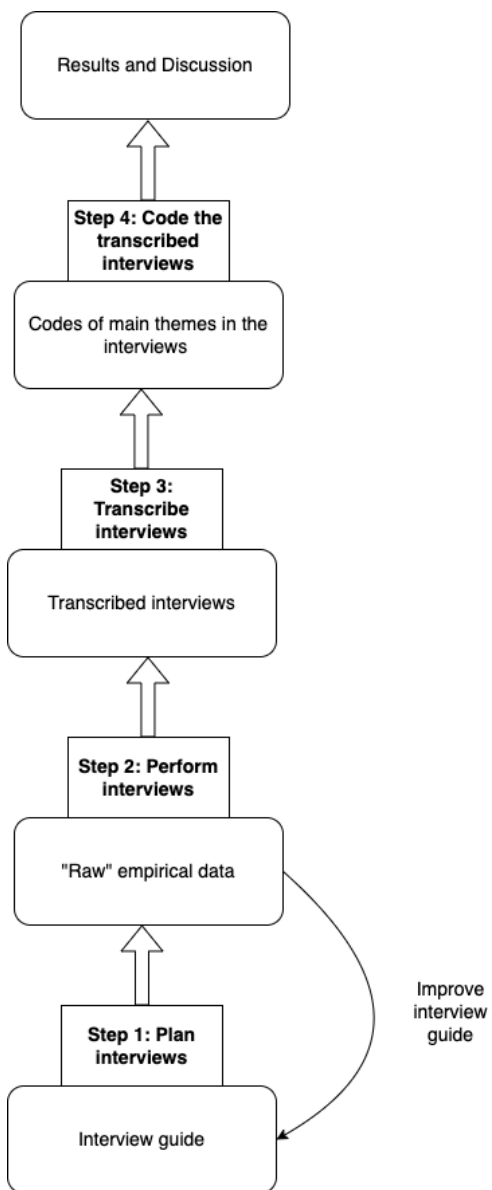


Figure 3.4: Step-wise inductive methodology, adapted from [75]

the interviewee thought about a topic, to paraphrase and present them in conjunction with the tables. We did this individually, dividing interviews between us, and marked quotes and paraphrases before switching and going through the interviews again. Furthermore, we made a comment on each marked phrase to indicate what code it represented, before we switched interviews and went through them again to check if we agreed with each other. After this, we entered Step Five and, using an Excel document, summarized the key points in the answers given by the interviewees so that we could compare them with other answers to find similarities and differences between them.

After this analysis, we started writing the results, dividing up different interviews and writing separately, which we were able to do because of the thorough processing we did in the previous phase. The results, combined with the background, served as a basis for the discussion. We worked together to define the main points we wanted to include in the discussion and then wrote individually, switching sections to check that we included the main points, and collaborated and talked about the parts where that were challenging.

3.5 Limitations

A limitation to the methodology is that not all interviews were coded using a coding tool. Only three of the interviews were processed using a coding tool, while the others were coded with colored highlighting and comments in a text editor. We chose to do it like this because we experienced that the less time-demanding color highlighting was sufficient after the first interviews. However, it could have been beneficial to apply the more extensive coding we used in the first interviews to all interviews to ensure that everything was coded satisfactorily.

Chapter 4

Results

In the following chapter the results and findings from the semi-structured interviews are presented. Prior to the findings, Section 4.1 introduces the interview objects and relevant information about them that has been gathered before and during the interviews. This is included in order to contextualize the statements, which we regard as necessary because semi-structured interviews need to be understood based on the experiences and perceptions of the interview object, not only what they explicitly say. The sequence of events in the cases is also presented for the social engineering victims. The sections are sorted and presented thematically, closely related to the coding strategy applied to the processing of the interviews that is described in Section 3.4.

Most of the subsection consists of a table that displays the most relevant quotes from the different interviewees to make the findings insightful yet compact and accessible for the reader. We also include paragraphs that present results in a paraphrased manner and explain the overall findings within the theme at hand.

4.1 Who are the interviewees?

This section provides an introduction of the interviewees and why their thoughts and experiences are relevant for this thesis. Havstad, Dahl, Lund and Jensen are not the real names of the interviewees, their names are pseudonymized for privacy. Gjære, Landsem, Fjellhøy, Verpe and Paulsen are real identities. In future sections the interviewees are referred to as *Security Expert A*, *Victim A* and so on. By doing so, it is easier for the reader to follow which kind of interviewee a statement comes from.

4.1.1 Security Experts

The security experts have different roles and work in different sectors. Security Expert A and B work in companies whose value proposition centers around information security, while Security Experts C, D and E work with security in organizations who have other objectives as their focus.

Security Expert A: Erlend Andreas Gjære

Gjære is a co-founder and the CEO of Secure Practice [62], a company that provides services to organizations for reporting of suspicious emails, security training and building a security culture within the organization. Gjære and Secure Practice particularly focus on how humans can go from being seen as the weakest link in a security chain, to being seen as security resources, in spite of the fact that 90% of all information security breaches can be attributed to human error, according to their homepage [62].



Figure 4.1: Erlend Andreas Gjære. The picture is sent and approved by Gjære.

Security expert B: Mia Landsem

Landsem works as a penetration tester in a security service provider company, and performs both technical and social engineering penetration tests. Therefore, she has experience with acting and thinking like an attacker. Landsem also works helping fraud victims in her spare time, and has figured in several news articles to discuss the consequences for the victim after these attacks [35], [33].



Figure 4.2: Mia Landsem. The picture is sent and approved by Landsem.

Security Expert C: Stig Henning Verpe

Verpe is the Chief Information Security Officer (CISO) in Sintef, a research organization in Norway. He works with establishing tools to protect Sintef's attack surface, entering agreements with security service providers, maintaining the knowledge and awareness of the employees, and developing the overall strategy for information security in the organization.



Figure 4.3: Stig Henning Verpe. The picture is sent and approved by Verpe.

Security expert D: Emil Havstad

Emil Havstad works as the Head of Digital Security in a public institution in Norway. He works with reacting to and preventing security incidents in all information systems related to the institution. A particular challenge in his organization is that a noticeable portion of the users are replaced with new ones on a regular basis, which makes long-term security training challenging. He describes a trend in the organization he represents where the number of attacks increases every year.



Figure 4.4: Illustration of Emil Havstad

Security Expert E: Jonas Dahl

Jonas Dahl works as an IT architect focusing on internal security strategies in an international company. He is a part of the response team when security incidents occur and maintains an overview of the current threat level.



Figure 4.5: Illustration of Jonas Dahl

4.1.2 Social engineering victims

Victim A: The University of Tromsø, represented by Odd Arne Paulsen

The University of Tromsø (UiT) is a public university in Norway [77]. As a public agency UiT is required by law to perform public procurement when purchasing services or products. This means that much of the information about potential transactions and contact persons is publicly available, which makes these organizations particularly susceptible to invoice fraud. In 2019 UiT decided to share publicly that the university had been exposed to a successful attack of this kind [52]. The interviewee, Odd Arne Paulsen, was not involved in the attack when it occurred, but acts as a spokesperson on behalf of the university and the involved employees when UiT presents information and discusses the attack.



Figure 4.6: Odd Arne Paulsen. The picture is sent and approved by Paulsen.

In 2019 UiT was going to buy a CT scanner, and a British supplier got the contract for the order. The supplier sent the invoice over email to the contact person at UiT, which is a standard procedure for foreign suppliers. The following day the same person at UiT received an email that seemingly was from the same supplier who asked when they could expect payment. The email domain was not from the supplier, but the UiT employee did not notice this, thus the BEC attack was in motion. The email contained a lot of information from the original invoice and provided a number of details that only were in the original invoice UiT received the day before. The UiT employee who received this email regarded it as a genuine inquiry from the actual supplier and answered in the same email thread. Then the "supplier" replied, asking if UiT could change the bank account number, and gave a credible explanation to why this was necessary, which included practical challenges with Brexit. After some internal discussion with other employees at UiT, where UiT requested and was provided documents from the "supplier" that confirmed the new bank account, UiT made the payment of 1.2 million Euros to the new bank account number. Weeks later, they discovered that they had transferred funds to the wrong account.

Victim B: Peter Lund

Peter Lund is a representative for a small service-providing company that, similarly to the employees at UiT, became a victim of invoice fraud caused by a spoofing attack. Unlike Paulsen, Lund prefers to keep his identity and details of the affected company anonymous. Among his day-to-day tasks at work, Lund is in contact with clients that buy services from his company, and he does not engage in work with security-related tasks himself in his job.

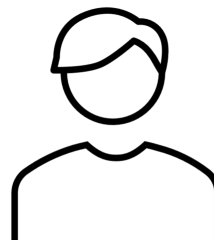


Figure 4.7: Illustration of Peter Lund

Lund and his client were victims of an invoicing fraud where the attackers intersected in the communication between Lund and the client. The attacker successfully fooled them in a typical spoofing manner where the email address and signature were consistent with other emails from Lund. We have access to these emails, but they are not included in the thesis to maintain confidentiality. Lund's company was supposed to receive payment from the client in two iterations. The first payment appeared in Lund's account as expected. Then the client received an email stating that Lund's company had a new bank account, and the client transferred the second payment to this account. During this process, both parties received emails from the other party that the sending party had not seen before.

After this, Lund and the client contacted the police, who started an investigation. Lund is not informed of further developments in the investigation, but received the missing payment from the client after some time. Thus, the client took the economic loss by first paying the fraudsters and then paying Lund's company.

For Lund, it is crucial that information about the case is not leaked, because this will negatively affect others in his company and their marketing strategy. As Lund describes, they have strict guidelines for what kind of publicity they want for the company, and this case compromises their strategy.

Victim D: Carl Jensen

Carl Jensen works in an IT company and fell for a security training test at his job in the form of a BEC attack. He received an email that looked like it was coming from the CEO of the company he works for, asking him to fill out a survey about the company's state and how the employees were feeling, providing a link to the survey. The company had sent out surveys like this before, and therefore, Jensen considered the email to be credible. The victim was happy about receiving the survey because he had some things he wanted to discuss regarding the company. Jensen remembers that he thought it was weird that the email said "Please answer by the 10th of February", while he received the email on exactly the 10th of February. Even though he found this strange, he still followed the link, which led him to a Microsoft Single Sign On (SSO) page. He disregarded another clue that could indicate something was wrong, and followed further instructions until he provided his username and password to the site and received a message saying he failed the security training.



Figure 4.8: Illustration of Carl Jensen

Victim C: Cecilie Fjellhøy

Fjellhøy is a UX designer working in London, where she also took her master's degree. In 2019 she went public with a story of how a professional social engineer had manipulated her for several months. She met the fraudster through Tinder, and started dating him under the impression that he was a wealthy businessman. After some time, they became a couple. Later on, he made her believe that he was in trouble and needed financial help from her, whereby Fjellhøy applied



Figure 4.9: Cecilie Fjellhøy. The picture is approved to use by the licensee.

for loans in nine different banks in Norway and the United Kingdom and provided him the money. It was after doing this she realized that he was a fraudster and reported him to the police. When she felt like the police did not do enough to solve the case, she told her story to the Norwegian newspaper VG, and has recurred in various news articles, as well as a documentary on Netflix. Since the incident, she has acted as a spokesperson for fraud victims claiming that banks, police, and other stakeholders are not helping her and other fraud victims sufficiently.

She is a victim of a different kind of social engineering attack than the other interviewed victims, because the scam relied on her falling in love with the fraudster so that he could exploit the trust she had for her boyfriend. Thus, this is not a case of phishing, spoofing, or BEC attacks, but Fjellhøy's story still covers topics that are relevant supplements to this thesis when it comes to the topics of shame, trust and transparency.

4.2 Results related to existing security economics theories

Results from the interview findings related to security economics theory are presented in this section. The results have been divided into different subsections, each expressing different aspects. The topics that are presented here are incentives, externalities and asymmetric information.

4.2.1 Incentives

As presented in Section 2.3, misaligned incentives can be an explanation to why social engineering attacks are successful. Within the topic of incentives, the interviews touched upon two main perspectives, namely when there are misaligned incentives between actors, as presented in Table 4.1, and when there are incentives to invest in security in Table 4.2. The statements regarding misaligned incentives in Table 4.1 are answers the interviewees gave when asked if they had any thoughts around how misaligned incentives between actors can influence the security in a system or between systems. This is question 11 in the interview guide in Appendix C. The following paragraphs presents other findings that the interviewees talked about relating to this topic, but that do not fit as statements.

Table 4.1: Statements from interviewees regarding how misaligned incentives between actors can influence the security in a system or between systems

Victim A	A-1	“When it comes to asking our supplier about whether or not they had been subjected to hacking or social engineering, we believe that we would not have received a credible response. We cannot trust the answer since they have a direct business interest in saying they were not affected by such activity.”
Victim C	A-2	“I feel that the banks can do so much more, but they have zero risk with keeping things the way they are”
Security Expert A	A-3	“Return On Investment (ROI) on security is always negative, because you ensure yourself against something that is supposed to not occur, and you never know if it would have occurred if you hadn’t made the investment.”
Security Expert E	A-4	“Many decision makers only talk money, then it is easy to not prioritize security. It is an optimization problem, it is stupid to spend money on security if attacks do not happen.”

Misaligned incentives were discussed by almost all interviewees, who had various ideas of how incentives are influencing the success of social engineering attacks. Some discussed the concept directly, while others touched upon it when discussing other topics.

In the context of Statement A-2, Victim C brought up that the banks have stronger economic incentives to make it easier to grant consumer loans, than they have ethical incentives to make it harder to get granted a loan in order to protect the customers from scams. She also mentioned that the banks face no economic risk themselves when involved in a scam. She explained that this is because if the bank grant a customer a consumer loan, it falls upon the customer to pay back the loan, even though they were tricked into establishing the loan. This is backed up by Security Expert B, who pointed out that although a perpetrator may be convicted of committing a social engineering attack where they make the victim apply for a loan, and the money goes to the perpetrator, the victim is often still left with the debt that has to be paid to the bank. Victim C argues that it would be beneficial to move the economic liability to the banks to align incentives better.

All the victims of social engineering that reported the incident to the police, Victim C, Victim B and Victim A, described challenges in their collaboration with the police that can be understood using misaligned incentives. One aspect mentioned by particularly Victim A and Victim C is that the police are not doing enough

for victims of scams. All of the victims experienced that parts of their cases were dropped by the police, despite existing trails of evidence. Furthermore, crimes that involve different police districts, such as Victim B, or go across borders, such as Victim C and Victim A, are described in the interviews as even harder to get the police to look into. Victim A indicates that international complications obstructed further investigation of the incident. Victim A also said that it is hard to discuss the reason of the incident with their supplier because the supplier had incentives not to disclose if they had been subjected to a security breach.

As Statements A-3 and A-4 shows, Security Expert A and Security Expert E brought up the challenge with investing in security. They both said that it is difficult to get people to invest in security because it protects against risks that are hard to measure, and therefore the decision makers that are in a position to implement measures that can prevent attacks may not have incentives to prioritize enough resources to this.

Table 4.2 shows statements from some of the security experts regarding various incentives different actors can have for investing in security.

Table 4.2: Statements on incentives for focusing on and investing in security

Security Expert A	B-1	“We have to protect our data. It severely affects our reputation if we get hacked because we are a trusted actor. We can’t afford to be hacked.”
Security Expert C	B-2	“Sintef has many customers, and is an attractive target. We can be used as a gateway into other organizations and it affects Sintef that they are being attacked because it affects Sintef’s reputation, we do not want a bad reputation at all. How Sintef is perceived externally is very important to us.”
Security Expert A	B-3	“In the end security boils down to asking ‘What are the priorities and goals of the business, also with regards to security work?’ Should the organization be compliant and not break the GDPR rules in order to avoid fines, or should we be forward-leaning and communicate that we are focusing in security, because we are a trusted actor, as in the case of my company.”
Security Expert A	B-4	“We have cyber insurance. Why? Because we get it very cheap.”
Security Expert A	B-5	“How do you sell security? This question is a challenge in the industry. How do you get someone to pay for something that has not happened?”

The security experts shared a common belief that investing in security is important to preserve the assets of their organizations. More specifically, they described how failure to invest in security can negatively affect their business, particularly due to loss of reputation. For Security Expert A, the business' value proposition is centered around security, which makes it particularly relevant to invest in security related assets. The same argument was also presented by Security Expert C, even though security is not Sintef's main value proposition. He argued that loss of reputation is one of the main incentives to invest in security mechanisms. Other goals the organization have can also serve as incentives to invest in security, as stated by Security Expert A in Statement B-5.

Security Expert C explains how Sintef regards employees as assets, and that helping the employees to be safe, both at work and in their personal lives, is considered important to Sintef's values, this is an incentive to put resources into learning employees about security. As Statement B-4 shows, Security Expert A also mentioned that a low price on security products and services can serve as incentives for investing in them.

4.2.2 Externalities

Having provided the interviewees with a definition of externalities along with some examples, we asked if they were aware of any examples of how externalities affect security within their organization. Table 4.3 shows the relevant answers to this question.

Table 4.3: Statements from interviewees regarding externalities

Security Expert A	C-1	“If you give a bad security advice, then it has a huge cost.”
Security Expert A	C-2	“Security fatigue can be viewed as an externality, it is a long tail of that, sort of like with climate change.”

As illustrated in Table 4.3 Security Expert A was the only one who gave a relevant answer when asked the question related to externalities. Security Expert A mentioned two different examples, as presented in Statements C-1 and C-2. Other interviewees tried to answer the question but did not give any relevant examples that could be categorized as externalities. Some of the interviewees said that they did not come up with any examples on this.

4.2.3 Asymmetric information can cause challenges regarding risk quantifying

Asymmetric information is a topic the interviewees were not asked about directly. Still, the subject was brought up by some of the interviewees when they were talking about ways to prioritize security resources and why they fell for an attack. These aspects related to asymmetric information mentioned by the interviewees are displayed in Table 4.4.

Table 4.4: Statements from interviewees regarding (asymmetric) information

Security Expert A	D-1	“I believe, from my own experience, that it is difficult to quantify risk.”
Security Expert A	D-2	“With cyber attacks, you have a motivated outsider trying to destroy for you, and you do not know what they are thinking, but you know that they are there and will strike. And then you become a bit like "what is the probability that they attack?”
Security Expert A	D-3	“Everything is based on you having an understanding of “What is the risk we face? What is most important for us to protect? ” If it can be quantified with numbers, or a gut feeling that we still agree on, then we end up with a collection of things that need to be fixed, then you have to prioritize them. ”
Victim A	D-4	“We probably have not had enough knowledge about the risk profile and have not been sufficiently aware of this kind of scam.”

Challenges with quantifying risks were discussed by Security Expert A as seen in Statements D-1 to D-3. Security Expert E mentioned that linking risks to non-economic factors such as growth, values, and reputation is challenging. Statement A-4 also mentions how he believed security is an optimization problem to a large degree due to uncertain risk. As Statement D-4 shows, Victim A argued that one of the reasons why they fell for the invoice fraud was because they did not have adequate knowledge of such attacks.

4.3 Interdisciplinary findings

This section presents results related to interdisciplinary findings. Each subsection focuses on either the challenges with countermeasures to social engineering in practice or attitudes towards social engineering.

4.3.1 Bad luck that a social engineering attack was successful?

Inspired by the findings in *Mørketallsundersøkelsen 2020*, presented in Section 2.1, we asked all the interviewees what they thought about whether or not luck or bad luck could be an explanation to why a social engineering attack was successful. Table 4.5 showcases some of the answers from a part of the interviewees, and as seen, there are different opinions on this matter.

Table 4.5: Statements from the interviewees about their thoughts whether luck is a reason to a successful social engineering attack

Victim D	E-1	“I don’t believe in luck, being lucky or unlucky. Circumstances yes, you might not have proper training, or you might not be aware, or have your thoughts in a different place. Throwing all this together might be called luck, but I think that there are a lot of factors playing at the same time.”
Security Expert C	E-2	“Sometimes people have a bad day and clicks when they do not usually do so. I do not disagree that it is bad luck. ”
Security Expert A	E-3	“I believe that it is because people in principle think that ‘This will not happen to me’, but then it happened to them anyways. The probability is technically speaking very low, you are one of five million people in Norway, so the odds of you being affected becomes low.”
Security Expert A	E-4	“We have a lot to learn from another concept, safety. Within aviation, process industry and health care. There we have longstanding traditions for safety, because it concerns people’s lives and health. In that case you never think of events as bad luck, because it is impossible to learn from bad luck. These are fields that have been developed generations longer than IT security. In these fields you always talk about <i>root cause analysis</i> . Ask the question Why several times when looking at how things happened. It’s never bad luck, and we have to learn to think like that in cyber security as well. ”
Security Expert B	E-5	“Bad luck concerns that they became the goal, but it is not bad luck that someone successfully attacked them, that is about not being prepared.”

Victim A	E-6	<p>“Blaming it on bad luck is a way to not take the blame. I do however think this is unwise because if it is luck then we might not be as motivated to make changes and take it serious enough to why this happened to your organization. It is an easy explanation that I do not think make you capable to prevent such an attack to happen again.”</p>
----------	-----	---

In most of the interviews, the interviewees agreed that bad luck is not the reason behind the success of social engineering attacks. Most of the interviewees believed that to blame it on bad luck would make it more challenging to uncover the root cause of the problem. An interesting finding is that one of the security experts, Security Expert C, said in the context of statement E-2 that he believed it could be bad luck sometimes that a social engineering attack succeeds. He stated that it could be bad luck that someone has a bad day and therefore clicks on a phishing email. Security Expert C also said that he believes it can be bad luck that you are one of the first to receive a phishing email in a phishing campaign. He elaborated that it would be easier not to fall for them if people had shared and warned about such attempts. Hence, it can be bad luck that you received such an email early in the "phishing campaign wave" and fell for it because no one warned you. Two other security experts, Security Expert A and Security Expert B, disagreed with Security Expert C, stating that successful social engineering attacks are not a result of the victim's bad luck. As Statement E-1 shows, Victim D neither believed that luck was a reason. Victim B said that he did not have any prerequisite to say anything about it.

Security Expert A also stated that if we blame a successful attack on bad luck or coincident, we will not learn the true reason why the attack was successful. Victim A expressed the same as Security Expert A that we will not find the true cause if we blame it on bad luck. Security Expert A states in Statement E-4 that we must ask the question why several times to find the root cause of why an attack succeeded.

4.3.2 Usability

When the interviewees were asked question 3 in the interview guide about why they think social engineering attacks are successful, some of the interviewees mentioned usability versus security as a topic. Table 4.6 shows some of the statements from interviewees who mentioned this topic as an answer to why social engineering attacks succeed.

Table 4.6: Statements regarding challenges with usability and how this can be a reason to why social engineering attacks are successful

Security Expert A	F-1	“How does security look from the user’s perspective? There are many separate security measures that altogether have accumulated to a lot of separate advice and demands. For example, to protect passwords we have requirements to achieve strong passwords, updating to new passwords and so on. From the user’s perspective this might feel like ‘Wow, now I am forced to do this’ which in many cases leads to frustration for the user.”
Security Expert C	F-2	“The more security mechanisms you have, the more hassle there is for the users. It’s not very popular when you put on constraints, so there’s a balance here. ”
Victim C	F-3	“There is often an intersection between usability and security, which also applies here considering how easy it is to get a loan.”

Security Expert A made a point out that he thinks technologists and engineers who have dominated the IT field have not always been aware of the user perspective and the usability of the technology that is being developed. Security Expert A said that he thinks it has made sense for engineers to make "security technology" to protect other technology, resulting in separate solutions that do not focus enough on people and how people use cyber systems. Security Expert A elaborated on statement F-1 and emphasized that if the security measures negatively affect the usability and make it troublesome, it can lead to *security fatigue* where people are tired of the security demands, and they will try to find less secure shortcuts. He stated that this lack of usability might be why social engineering is as successful as it is. Security Expert C expressed the same beliefs as Security Expert A, and as he stated in Statement F-2, he believed users get annoyed if there are many security mechanisms. Victim C, on the other hand, talked about how she thought there is too much focus on usability, especially in online banks. She meant security and control mechanisms should play a more significant part in the workflow of applications and processes to protect users from social engineering better. She stated that it would not be negative to prioritize security and control mechanisms over usability. Furthermore, she said that a part of the reason why this is not done is that banks have economic incentives to grant users loans, as presented in Section 4.2.1.

4.3.3 Shame

Shame was not a topic we asked about during the interviews, but some of the interviewees brought up the topic. Victim C said that one of the reasons she was

open in the media about being scammed was to help other victims of similar scams by showing that it is not embarrassing to be tricked by professionals. She said she wants to show others in similar situations that they are not alone, and she wants to reduce the shame of falling for social engineering. She described that she thinks a lot of the shame around social engineering scams comes from not being seen as a victim by the police or others or not being treated well. Victim C expressed that if the police confirm this initial shame, victims may have felt it may cause them not to dare to be open about the incident. Security Expert B also expressed that many people who fall for social engineering feel shame about being scammed.

Victim A said that UiT has focused on not blaming and shaming individuals for the mistake around the invoice fraud and instead focusing on the organizational learning and what they need to do differently to avoid similar incidents. Security Expert D said that the organization he works for has tried to reduce the shame around falling for phishing emails. Moreover, he emphasized that everyone can be fooled and that it has to be room to make such mistakes without being shamed for it.

4.3.4 Challenges with security training

During the interviews some of the interviewees pointed out that security training may not be such an effective measure to hinder social engineering attacks. Table 4.7 displays statements of what have been highlighted related to this topic.

Table 4.7: Statements regarding challenges with security training

Security Expert C	G-1	“We notice that people are very unhappy and think it is a waste of time, while others think it is very good to be tested. It is hard to make everyone happy.”
Security Expert A	G-2	“I think that it is a hopeless advice to "be skeptical of emails, don't click on links or open attachments".”
Security Expert C	G-3	“It is difficult to maintain, no one bothers to watch the security videos over again.”

In addition to saying that much security advice given during security training is hopeless, Security Expert A also highlighted the lack of pedagogy in many security training programs, which he meant is hindering the learning. Security training also poses a challenge in what the management aims to achieve when deciding whether to provide employees with security training, Security Expert A claimed. He said that if the security training was only compliance driven, and the management only cared about checking off that the employees have gone through a form of security training, then it may be that the training did not raise as much awareness as it

should. Another challenge with security training Security Expert C highlighted in Statement G-3 is that people tend to fade out security awareness campaigns. Security Expert C also expressed that running phishing simulations on employees is perceived differently among the employees, as Statement G-1 expresses.

Both Security Expert B, Security Expert A, and Security Expert C also mentioned that it is challenging to have generic security training that fits everyone because there are different security awareness levels internally in an organization. This makes it challenging to find an efficient level that will make the training purposeful for everyone. Security Expert B also mentioned that we have gotten so used to generic and bad phishing emails that when a social engineering attack is sophisticated and targeted, it is difficult to discover because we expect social engineering attempts to be unsophisticated and generic.

4.3.5 Trust

Several of the interviewees discussed the concept of trust as an important aspect related to social engineering. Trust was not asked about directly, but some interviewees mentioned the topic. Table 4.8 shows some important statements on this matter.

Table 4.8: Statements from interviewees regarding trust

Victim C	H-1	“I think trust is a beautiful and good thing we have in Norway”
Security Expert B	H-2	“Older ladies do actually understand that love scams are not real, but they do not want to realize that people are so evil.”

A recurring explanation from the interviews as to why people generally fall for social engineering attacks is that people want to be helpful to people they trust. According to Security Expert C, this behavior can lead people to do things they should not do, which leads to a less secure environment. Security Expert C’s statement matches what Victim C said about the kind of people who fall for similar scams as her. She said that most of her fellow victims easily trust people and want to help out when someone needs them. Even though Victim C trusted the attacker and fell for the scam, she still meant that trust is a good thing and that the trust in Norway is positive. Even though she has suffered substantial economic losses, she still trusts people. She expressed that this is because what happened to her was very special, and her life would be destroyed if she had to be skeptical about every person in her life. Security Expert A stated that he does not want to "kill the trust in Norway"

but that it is essential to focus on that the person you are talking with is the one he is claiming to be.

Victim A mentioned that trust might also be a security issue when it comes to trusting the assessments of your co-workers. This is seen as one of the reasons why UiT fell for the attack. When the recipient of the fraudulent email forwarded the email to other employees for processing, the other employees assumed that the first recipient had done a thorough enough job of checking the validity of the email. Hence, no questions were asked by the others because, according to Victim A, they trusted their co-workers too much.

Transparency

In the interviews, all the interviewees mentioned the importance of being open and transparent about security incidents and that this can reduce successful social engineering attacks due to increased awareness and available information. However, getting people to discuss security incidents is more complicated. Transparency was not asked about directly to the security experts; they brought up the topic themselves. The victims were asked about their opinions regarding transparency related to social engineering attacks and why they chose to or chose not to be transparent about their case. The most important statements from the interviewees are presented as statements in Table 4.9.

Table 4.9: Statements from interviewees regarding transparency of security incidents

Security Expert C	I-1	“Being open about what works and what happens, why things have happened, that is a good effect, because it is something everyone can learn from. Many people are very careful about going out with things that have happened because they can assume that others then do not want their data there because it is poor security. But the truth is that everyone has challenges and everyone certainly has a breach of either policy or other security systems, so being open about it is a huge advantage.”
Victim B	I-2	“It is important that this incident does not end up in the media.”
Victim B	I-3	“I think it would be useful to talk about this incident.”
Victim A	I-4	“We cooperate in our sector, and have a good collaboration with the university-sector. We share information regularly.”

Due to the fear of negative media attention the security incident Victim B was involved in could cause for his employer, Victim B is apprehensive about what happens if people hear about this incident. Therefore, he strives to keep it secret and out of the media's attention. Despite withholding his story from the public, he believed that being open about incidents like this would generally be helpful for others. UiT, on the other hand, chose to be open about the security incident even though they too believed it would negatively impact the reputation of the university. Victim A, however, said that there had not been much direct criticism towards the university after sharing details of this incident. He also stated that he has experienced a certain acceptance that it is possible to be deceived, and that the victims do not have all of the blame, even though the incident still negatively affects the reputation. Despite knowing the incident could harm its reputation, UiT went public with it because of the external and internal benefits of being open about it could cause. According to Victim A, awareness is the key to preventing attacks like this from happening repeatedly. Furthermore, he expressed that it can reduce the chances of successful attacks when being transparent, and as stated in Statement I-4 he said that they cooperate in the sector.

Victim C said that transparency about being subjected to a social engineering attack hopefully can reduce the shame around being a victim of such attacks, further described in Section 4.3.3. It is essential for her to be open about her experiences because she hopes it will prevent similar incidents and make the process after a successful scam easier to handle for future victims.

Victim A stated that he is critical to all the publicly available information in the public procurement databases. He said that this is a goldmine for those who wants to execute a social engineering attack.

Security Expert C had similar opinions as Victim A about the positive effects being open about security incidents can cause, as presented in Statement I-1. He informed that the organization he works for shares information about security incidents and tips about countermeasures that work for them in various fora. Security Expert A also expressed that we should be open about security incidents, both internal in the organization, so the incident can be handled as quickly as possible and externally so that others can be aware of similar attacks. Security Expert A mentioned that it is important to have an organizational culture where individuals do not get blamed for falling for social engineering attacks. He stated that this could lead to employees not wanting to be transparent and share when they have clicked on a phishing link.

Culture

Security experts A, C, E and Victim A highlighted culture as an essential part of why social engineering attacks are successful and how security culture can reduce

successful attacks. In other interviews, the interviewees did not mention the theme at all, and were not asked about it because questions about culture were added in the interview guide when we found the topic important. This was after some of the interviews had already been performed. Table 4.10 presents statements about security culture.

Table 4.10: Statements from interviewees regarding security culture

Security Expert A	J-1	“Then there’s culture, which can be an externality. The more people you convert to the security team, the harder it becomes to not be a part of this team. If the "old crab" who doesn’t like security feels like he’s on the outside, you have gotten a bit further.”
Security Expert E	J-2	“The company doesn’t use name tags, this is actually a security risk, but we don’t want to implement this because it makes the company feel a lot bigger, and this goes against our company culture. ”
Security Expert E	J-3	“Most of the prevention of social engineering attacks is because the employees know each other and they talk together, so they do not fall for scam emails like that.”
Security Expert A	J-4	“First you need to come up with measures that make sense to people. It is difficult to build a culture based on coercion and duties.”
Security Expert A	J-5	“People find ways around strict security policies if they become too demanding, and then you get a negative culture where people don’t care about policy, because the policy isn’t seen as feasible. It is demanding, you have to make an effort instead of simply saying that ‘The policy is like that, so we do it that way’. Then you wind up with a bad policy, that leads people to not caring as much about what you say, and you get a worse security culture.”

Statement J-2 in Table 4.10 expresses that organizations can be willing to accept security risks if the countermeasure to the risk does not match the organizational culture. Furthermore, as Security Expert A expressed in statements J-4 and J-5, the security policies and measures cannot be too demanding; thus, this will create a negative security culture. Victim A also mentioned that they had a very trusting culture, where employees trusted that others had checked validity of inquires. Security

Expert A and Security Expert C also highlighted the value of empowering users and giving them a sense of achievement when dealing with security issues. According to Security Expert A, nurturing a feeling of accomplishment and digital confidence among users will motivate them to go further in their day-to-day security routines.

4.3.6 Other findings

This section presents interview findings and perspectives that did not fit well into a category but which are important. Table 4.11 shows some of these statements. The statements are related to questions of why the interviewees think security measures not always work in practice.

Table 4.11: Statements on additional findings on why security measures fail in reality

Security Expert A	K-1	“From the defense side we have been sufficiently good with regards to technology, but maybe not when it comes to understanding people. I think that is an important reason why social engineering works, because we have focused on the wrong things.”
Security Expert C	K-2	“Many use "shadow-IT" in their organization, they use private systems such as Dropbox to move corporate data. It is very common to do things in an easy way.”
Security Expert C	K-3	“People are going to do things quickly and be helpful, which means that they may not think thoroughly enough in the moment.”
Security Expert B	K-4	“We receive spam emails all the time, so we think that it is easy to detect them, thus when such emails become professional it is hard to detect because we are used to it being so easy to notice spam emails. It may be that we are not so observant of emails when it is done professionally because we are used to this being done badly.”
Security Expert B	K-5	“We cannot avoid clicking on all links.”
Victim B	K-6	“Before the incident happened I was probably more like most others, I thought; no this does not happen to me, I see it in the newspaper, but it does not apply to me. How stupid are those who falls for something like that.”

Table 4.11 visits many topics, but the common theme is the same; why things fail

in practice. In addition to the statements, Security Expert A also mentioned that certain policies that sound smart in theory might not work in practice. He gives an example of verifying account numbers by calling the bank before making a payment may seem like a good policy that could hinder social engineering attacks. However, this would not be possible in practice due to time constraints and efficiency.

4.4 Humans as the weakest link

As mentioned, the claim that humans are the weakest link in a security chain has been widely accepted and established. Table 4.12 shows what some of the interviewees mean about this claim.

Table 4.12: Humans being or not being the weakest link

Security Expert C	L-1	“In the end, everyone gets tricked. ”
Security Expert C	L-2	“The advantage humans have that machines do not have is their gut feeling, humans can flag things that the technical cannot.”
Security Expert A	L-3	“If humans are the weakest link, then humans are the least utilized security resource. Instead of deleting spam emails, you can use them to find out what’s going on.”
Security Expert E	L-4	“Humans are the weakest link, but not because they are stupid. There is always intentional gaps in the security. We cannot block all attachments, addresses and such because the problem is that if you block too much, you loose valuable information.”
Victim D	L-6	“I do not think I am the weakest link. I might be the weakest link if you implement the recommended security procedures, but I think there are weaker links with the things we’re doing than myself, because we are not following best practices everywhere. If you were to adhere to best practices I would say “yes, I am the weakest link, because I am the easiest thing to exploit outside really sophisticated attacks”. But I think there are other things that are weak links as well, because not every area of what we’re doing is up to speed. ”

Victim C	L-7	“I don’t think it is correct that humans are the weakest link, because if things had not been so automated, and I had been forced to talk with someone in the bank and things had taken more time, it probably wouldn’t have ended as badly as it did for me.”
Victim A	L-8	“I would probably agree with that, given that you have a minimum of security mechanisms and not everyone have full access to everything, but that authentication and verification are required to a certain extent. But then it comes back to the point that there are people who have to do these things in order for things to go wrong.”
Victim B	L-9	“I agree with the assertion that humans are the weakest link.”
Victim A	L-10	“I believe that the human factor is important and that we have not been aware enough of this, not been careful enough or had sufficient competence. Our people were fooled when they should not have been. They should have seen that the email came from another address, and asked more critical questions.”

As the statements in Table 4.12 illustrate, the interviewees have different opinions on the matter. Victim A, Victim D, and Security Expert E all expressed that humans are the weakest link if all the recommended security procedures are implemented, but if this is not the case, they all stated that they do not think humans are the weakest link. Security Expert A also disagreed that humans are the weakest link, and both he and Security Expert C stated that a significant advantage with humans is our gut feeling that can catch things machines cannot. However, contrary to Security Expert A, Security Expert C did not specifically say whether or not he agreed with the statement. Security Expert C instead elaborated that it is people who click on links and download attachments in the end. He further said that one of the reasons we fall for social engineering attacks can be dependent on the day-to-day form and that we are more receptive to things if we are interested in a subject.

Victim B and Victim C have different opinions than the two other victims, Victim D and Victim A. Victim B agrees with the claim that humans are the weakest link, and he argues that he thinks humans are too inattentive. In contrast, Victim C disagrees with the statement and argues that automation has more blame than humans.

4.5 Protection against social engineering attacks

This section presents suggestions given by the interviewees against social engineering attacks. Note that all of these are not new recommendations, but things the interviewees meant are important to focus on. The interviewees mentioned most of these recommendations when asked about questions relating to which countermeasures they believe are useful against social engineering attacks.

4.5.1 Security awareness improvements

As mentioned in Section 4.3.4, some interviewees expressed that they did not think security training was effective enough. Some of the interviewees gave recommendations on how they thought security training could be improved. These statements are presented in Table 4.13.

Table 4.13: Statements on security awareness improvements recommendations

Security Expert C	M-1	“It is good to have recurring security campaigns because it raises the awareness of people, people tend to fade out security campaigns. ”
Security Expert A	M-2	“Give people a tool that makes security seem manageable.”
Victim A	M-3	“Awareness, competence and vigilance of social engineering and different methods used in social engineering and knowledge of what one may actually be exposed to is what can help making such attacks less successful. It is not enough to have a vague feeling that fraud exists.”
Security Expert B	M-4	“Get to know the applications. I know for instance that Meta would not call me, but most people do not know of such processes.”

Security Expert C described that people’s awareness after completing security training quickly fades. Therefore, concerning Statement M-1, Security Expert C said that recurring security campaigns instead of one training that covers everything at once could help. Security Expert C also mentioned that in big organizations, the security competence might vary largely. Thus, he meant it would have been useful to have level-based security training. Security Expert A believed that security training can be improved by focusing more on usability. He suggested that pedagogy plays a more significant part in security training to make the training more effective. Security Expert E expressed, similar to Security Expert A, that security training

is not valuable enough and that we need to improve the training to get people to interact.

With reference to Statement M-2, Security Expert A stated that boosting people’s digital confidence and making them believe that security is something they can master and learn rather than believing that it is so complicated that they cannot prevent it can reduce successful attacks. Victim A, on the other hand, believed that focusing not only on countermeasures against social engineering attacks, but also learning about how attackers attempt to attack and scam can reduce successful attacks. Security Expert B recommended that users increase their knowledge about the applications they use.

4.5.2 Technical measures

The interviewees also mentioned that technical measures could reduce social engineering attacks. Table 4.14 provides an overview of the technical recommendations from the interviewees.

Table 4.14: Statements on how social engineering attacks can be reduced by technical measures

Security Expert C	N-2	“Everyone should have signed emails”
Victim D	N-3	“Implement a warning that alerts if an email comes from outside the organization.”
Security Expert D	N-4	“There should be several security layers, username and password should not be the only thing you need to enter the system, two factor authentication is important.”
Security Expert C	N-5	“Have a built in reporting mechanism connected to your email, so you can report suspicious emails.”

Security Expert B said that there are no technical measures against social engineering. In contrast, all the other security experts we interviewed said that good technical protection is essential, making it more difficult for attackers. For example, interviewees recommended email signatures, DMARC, notifications if emails are sent from outside of the organization, and two-factor authentication in case someone has gotten a hold of a password. In addition, both Security Expert A and Security Expert C recommended having a built-in email reporting mechanism for the IT department, for instance, in the email service, so we can leverage the human gut feeling to filter out suspicious emails. Such a reporting mechanism that automatically sends an alert to someone that can check the email or scan the email for malicious code can, according to Security Expert C and Security Expert A, lower the threshold for checking suspicious emails before clicking on them.

4.5.3 Attitude change

The recommendations in this section address attitude changes. There were no questions directly related to this topic, but it was mentioned when the interviewees talked freely. Table 4.15 shows some recommendations related to attitude changes.

Table 4.15: Statements on how social engineering attacks can be reduced by attitude change

Security Expert A	O-1	“We have to work with giving people a sense of mastery and success, and that they can "do it". This moves, if not the responsibility, but the empowerment over to the user, so they are able to do more than just being skeptical.”
Security Expert A	O-2	“Take security from something that is boring, troublesome, difficult and dangerous to something easy and user-friendly.”
Security Expert A	O-3	“It probably sits a bit in the walls that IT people make you feel a little stupid. This makes people dread asking because it becomes a bit scary. Receive people with understanding and respect so that people feel it is better to ask for something instead of taking a chance.”

To get people to be aware and focus on social engineering countermeasures, which will reduce the number of successful attacks, Security Expert A recommended making people believe that these countermeasures are doable. Security Expert A also said that he believe an attitude change by IT people is necessary because only the attackers win when people are scared to ask IT personnel for help and advice.

As mentioned in Section 4.3.3, Victim C stated that she thinks it is crucial that the police change their attitude towards victims and focus on not shaming and blaming them. She said that being shamed by the police and others results in people not daring to be transparent and open about security incidents. Victim C also said that she wants the banks to take more responsibility.

4.5.4 Building a good security culture

Building a good security culture within an organization was another topic that some interviewees brought up when asked about which measures could reduce the number of successful attacks. Table 4.16 shows some of the statements concerning this.

As seen in Table 4.16 recommendations include all from having a culture that promotes transparency to striving for the best security we can. As Statement P-2 shows, Victim D suggested that security should concern everyone in an organization.

Table 4.16: Statements on how social engineering attacks can be reduced by building a good security culture

Security Expert A	P-1	“There should be transparency and a culture where it feels safe to talk about mistakes.”
Victim D	P-2	“I believe that dedicated resources are not the solution to the problem. In my opinion they might be a part of it, you might have someone who has a very heavy security focus, but I believe, similar to proper DevOps-culture, that it is a concern that needs to be handled by everyone within your engineering organization. ”
Victim D	P-3	“Empower people in the organization to strive for the best of class engineering, and that includes security.”

4.5.5 Policies

Table 4.17 shows different suggestions on how policies can reduce successful social engineering attacks. These suggestions were also given based on the question concerning which measures could reduce successful social engineering attacks.

Table 4.17: Statements on how social engineering attacks can be reduced by policy measures

Security Expert C	Q-1	“When someone changes the invoice number, there is a requirement for a check by phone, so it is a process around changes to payments, where there must be separate procedures.”
Security Expert C	Q-2	“We have asked employees not to use the email for private purposes, so if there is an email from Telenor or the bank, they know that it is spam because everything private will come to another email.”
Victim C	Q-3	“The bigger the consequences are for you as a private person, the more manual elements should be included in the process.”
Victim A	Q-4	“Use an independent verification channel. Go back to the original and established way of communicating with the supplier and ask for confirmation if inquiries are received in a different way.”

Both Security Expert C and Victim A agreed that an independent verification channel would help reduce attacks. This recommendation was given in the context of invoice fraud. As Statement Q-3 shows, Victim C said she thought less automation in banks could be useful and could reduce successful attacks or the consequences of attacks. She elaborated that extra verification when doing larger bank transfers than usual could be a valuable policy for the banks to implement. Security Expert C said as Statement Q-2 presents that they have a policy in their organization concerning that employees should not use the organizational email for private purposes, which is something he suggested can reduce successful social engineering attacks.

4.5.6 Costs related to countermeasures

Table 4.18 shows that Security Expert A and Victim A meant that in order for countermeasures to actually be implemented and be useful, it is important to consider the cost of the countermeasure to the risk of an attack. This topic was brought up when they talked about which countermeasures could be useful to prevent social engineering attacks.

Table 4.18: Statements on how costs related to countermeasures against social engineering attacks

Victim A	R-1	“I think a risk based approach is important when talking about countermeasures for social engineering, there is also costs related to such measures.”
Security Expert A	R-2	“Good routines and policies are important, but they need to reflect the risk level.”

As Statements R-1 and R-2 show, Security Expert C and Security Expert A suggested that countermeasures need to reflect the risk level. Furthermore, they both emphasized that countermeasures cannot be overwhelming and that organizations do not have unlimited resources to spend on measures against social engineering.

Chapter 5

Discussion

Chapter 5 is a discussion about the findings from the interviews presented in Chapter 4, and how these findings can provide insight to the research questions, using background from Chapter 2 whenever suitable. This chapter is organized in a manner where all research questions are discussed in separate sections, from Section 5.1 to Section 5.4. This is followed by a presentation of known limitations in Section 5.5.

5.1 Research Question 1: Security economics in social engineering attacks

In this section, we discuss Research Question 1 and look at how the existing literature about security economics contributes to understanding why phishing, spoofing, and BEC attacks are successful and to what extent findings from the interviews align with or deviate from the existing literature. The love scam Victim C was involved in is also discussed even though this is not a phishing, spoofing, or BEC attack, because the experiences are valuable and can be applied to other social engineering attacks as well. In addition, the findings from the BEC and spoofing cases might also apply to other kinds of social engineering attacks. However, BEC, spoofing, and phishing attacks, along with the love scam regarding Victim C, are the focus of this discussion.

Getting people to share their experiences about falling for social engineering attacks was a big challenge. Therefore, we performed interviews with all victims of social engineering attacks that wanted to talk to us to gather enough data. Unfortunately, we did not find anyone that wanted to share their experience with a successful phishing attack. However, the security experts discussed phishing attacks in the interviews, which provided helpful insight. We also regard many of the findings from the BEC and spoofing attacks to be relevant to phishing attacks, and therefore we argue that we still have grounds to discuss phishing attacks.

5.1.1 Misaligned incentives create a dynamic where issues are not properly dealt with

The interviews provided various findings that relate to incentives and misalignment of these, which are discussed in this section.

Currently, in Norway the private persons that fall for social engineering scams are the economically liable actors, and they face the economic effects of successful attacks [1]. This is because the banks are only responsible for covering the loss if it is caused by unauthorized transactions, and the transactions in these attacks are normally authorized by the victims themselves. However, according to Ross Anderson this makes the banks careless, which leads to a more significant number of successful scams, as presented in Section 2.3.1. Victim C's statements about the trade-off between usability and security substantiate this. Currently, the banks have strong incentives for having smooth solutions with high usability to maintain and increase their customer base. The security challenges related to usability are further discussed in Section 5.2.1 while in this section we discuss how usability affects incentives. Victim C states in Statement A-2 that banks have very few incentives to prioritize increased security above more usability when it comes to bank transfers and consumer loan grants. As presented in Section 2.3.2, this trade-off can result in misaligned incentives, because decision makers can choose the alternative that is less optimal for society. We believe banks could implement more policies and features which could be helpful for people who are subjected to attacks. One such example is presented in Section 5.4.1. Improved financial liability alignment might help motivate the banks to perform actions that reduce the risk of successful attacks.

Most of the victims, except Victim D, talked about challenges with the processes with the police, as mentioned in 4.2.1, and validated the frustrations described by other victims in Section 2.1.4 [74, 59, 73], about cases being dismissed entirely or partially. When it comes to cases of social engineering attacks, these challenges become even more complicated because the fraudsters can fool many individuals for smaller amounts of money or other confidential information, making each successful transaction less attractive for the police to prioritize. From the police's perspective, these prioritizations can make sense because the resources needed might yield better results if invested elsewhere, as well as working across international borders can be an additional challenge for the police. However, the consequence of not prioritizing these cases is that the adversaries know that the risk of being caught is low, making the potential payoff worth the risk, thus creating more incentives to do so. Limited capacity of the government and small chances of being caught is also something Baddely argues for [12], as presented in Section 2.3.2.

Another challenge brought up by Security Expert E and Security Expert A was getting people, especially decision-makers, to invest in security measures. They

argued that investing in security is just an expense for most organizations. It will not make the organization any money, so the question is which incentives exist for investing in security. For example, suppose the attitude of the decision makers is that humans are the weakest link or that falling for a BEC, spoofing, or phishing attack is because of bad luck. In that case, it may be hard to find incentives to invest in social engineering measures since it appears that resources should be allocated elsewhere when humans are the weakest link no matter what. Despite this, the concept that humans are the weakest link can serve as an incentive to enforce security training and policies to minimize misbehavior. Other incentives to invest in security can be the fear of getting a bad reputation, as mentioned by several of the interviewees, as well as the organization might want to market that they follow security standards and best practices. Even though such a compliance-based approach to security can serve as incentives to invest in security measures, it might not be the best approach as Security Expert A argues. Moore also argues that compliance based security approaches are prone to fail, as mentioned in Section 2.3.2.

Another challenge with getting people to invest in security is that it can be challenging to decide how much resources to allocate because the risk of security breaches is unknown. This challenge can create misaligned incentives for decision-makers; the uncertainty can result in resources being spent on different matters.

5.1.2 New perspectives regarding externalities

In *Why Information Security is Hard - An economic perspective* [8], Ross Anderson highlight how network externalities and the value of cooperation with complementary assets aid to explain why security is neglected. However, the definition of externalities proposed in Section 2.3 can include a variety of other concepts as well. During the interviews, a few such concepts surfaced, and in the following section, we describe these concepts, and argue why they should be included when discussing externalities in security economics.

One such example found during the interviews is the fact that employees have to spend a lot of time dealing with security such as wondering whether emails etc are safe. This can lead to the company losing money and market share because the employees spend less time on things that can create revenue for the organization.

Transparency

Transparency is something the interviewees emphasized as essential concerning social engineering. The interviewees did not describe particularly what the value of transparency is to them, but shared the understanding that transparency is important to circumvent successful social engineering attacks. Some of the interviewees described various fora where they share security cases with others within the same industry

sector, as stated by Victim A in Statement I-4, and thus already strive to reap the fruits of shared information.

Some of the benefits of transparency have been described in previous papers, such as improved probability estimates for decision-makers, as described under **Information sharing** in Section 2.3.2. During the interviews, we discovered several additional effects transparency has on security, which we regard as important for further discussions about social engineering. One of the main takeaways from the processing of the interviews is that transparency should be regarded as an externality when discussing social engineering from a security economic perspective. This is because increased transparency provides increased insights in how we can learn more about these attacks, and thus protect ourselves better. Transparency about social engineering incidents should be considered a public good within information security. An argument for this is that the information is non-excludable because transparent information is available to everyone, and non-rival since no single person's use of this information excludes other people's use of the information.

To be transparent about a social engineering security breach will not necessarily benefit the victim organization, but another organization will potentially be more equipped to prevent an attack they have learned about from others. We gather that increased knowledge about incidents can improve the behavior of not only decision-makers that calculate probabilities, as presented in Section 2.2.1, but also users who can react more effectively when exposed to an attack if they have knowledge of similar attacks in other organizations. Furthermore, more transparency results in better estimates of how many attempted and successful attacks there are globally. This can reduce the amount of dark figures, and improve the public understanding of how exposed we are to these attacks.

Moreover, we found valuable insight in the cases where the interviewees disagree. The most evident of these inconsistencies are found when comparing Victim B and Victim A's interviews. Both parties supported transparency as an ideal to improve security. However, unlike Victim A at UiT, Victim B prioritized his employer's need for secrecy above the benefits the public receives from increased transparency. This indicates that there are not only positive effects of being transparent. From the interviews we conclude that one negative effect of transparency is loss of reputation, which negatively affects the attacked organization more than the positive externalities from increased transparency. Victim B explained that for his organization the need for secrecy does not rise from fearing a loss of reputation. It comes because of the marketing strategy in the organization, where they strive to avoid any news, good or bad, that do not discuss the organization's value proposition. This is an example of how a moral hazard is manifested in the battle against social engineering attacks, because each actor benefits from being selfish and withhold information that

can negatively affect their reputation, even though society as a whole benefits from increased transparency. It also shows how transparency as a public good is exposed to the free rider problem described by Baddeley in Section 2.3.1, where one actor benefits from the transparency of others, without exposing themselves to the costs related to doing the same thing. Victim A also shared his doubts about everyone being transparent about security breaches. He did not believe their supplier would be honest and share whether or not they had a security breach because they had incentives not to be transparent, as presented in Section 4.2.1 in Statement A-1.

Culture

We believe culture is a new relation to the security economics field that is important to include in order to gain a better understanding over how to protect against social engineering attacks. We conclude that culture should be viewed as an externality. Security Expert A expressed in Statement J-1 that he also believes culture should be regarded as an externality. An argument supporting this is that the more people who care about security and focus on including security in the culture, will cause the security focus to spread throughout an organization. From the interviews we conclude that it will be harder to resist security policies and awareness focus if this is a part of the culture in an organization, and easier to ignore if it is not an integrated part of the culture. An example given in the interview with Security Expert A is that if many of the employees in an organization turn off two factor authentication, because they find it annoying, it will easily spread throughout the organization. If a new employee asks how to deal with two factor authentication and is told that "everyone turns it off", it easy to follow this. It is harder to go against the flow, than to flow with it. Hence, focus on making security a part of the organizational culture can help reduce successful social engineering attacks, as well as other security breaches. Nonetheless, the free rider problem as described over, also relates to when security is a part of the organizational culture.

However, the interview findings show that it is important to align the security culture with the organizational culture to succeed with security. Otherwise, it is more tempting for people to find ways to go around security measures and not always follow security policies. For example, as Security Expert E mentioned, they have chosen not to use name tags in his company even though this makes them more vulnerable to social engineering, where people walk in and pretend to work there. This is a conscious choice by the organization. They appraise the organizational culture as a higher utility than the reduced security risk because an essential part of their culture is that the company is intimate enough so that everyone knows each other. The name tags would make the company appear larger and create the illusion that people do not know each other.

5.1.3 Decision making is challenged by asymmetric information

Because the concepts of misaligned incentives, externalities, and asymmetric information were rather unknown to the interviewees, we chose not to ask about the last of these concepts directly. Instead, we analyzed the interviewees' statements and saw if they mentioned something related to asymmetric information.

One such thing was that it is difficult to quantify risk. As pointed out, this is challenging because factors that affect the risk are the attacker, the ways attackers operate, and values like reputation and growth are hard to quantify. From the interviewees we gather that not having enough information about the threat landscape and the different methods attackers uses, and the risk we faces affect how organizations regard social engineering risks. Limited information about security attacks and breaches and the different demonstration of statistics, as presented in Section 2.3.1, helps amplify the uncertainty regarding risks. Decision making is also affected by probability estimates. Before the spoofing attack happened to Victim B, he did not think about security during his work. He never regarded social engineering attacks as likely to happen to him, and as mentioned he thought that it would not happen to him. After he felt victim for the attack he said that he now is very conscious of any suspicious emails and people trying to scam him, and that he sends them to an IT department right away. This is an example of the availability heuristic, as presented in Section 2.3.1. Victim B now assigns higher probabilities to being affected by a social engineering attack, then what he did before the attack.

5.2 RQ2: Theoretical solutions in reality

Throughout the interviews, it became clear that there are several explanations for why the theoretically secure solutions that can protect against social engineering attacks fail in practice. The following subsections discuss explanations given by the interviewees.

5.2.1 Trade-offs between different needs

Usability versus security

A few people discussed usability versus security during the interviews, and there are different opinions on whether or not security mechanisms should be weighed more than usability or not. Of all of the interviewees that mentioned this theme, Victim C was the only one who said that she thinks there is too much focus on usability that down-prioritizes security, especially in conjunction with bank ID and digital loan applications. In the incident she was involved in, a big part of the economic consequences she experienced were related to loans, so it makes sense that she wants more robust policies and security mechanisms related to these processes.

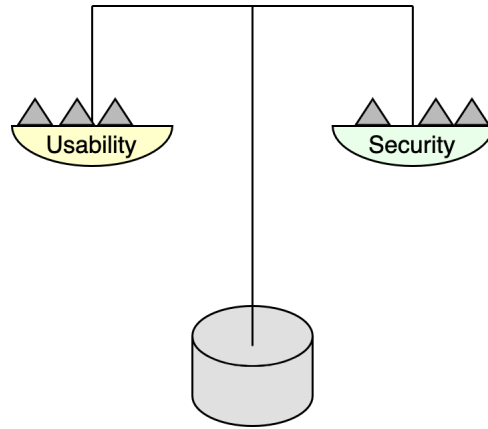


Figure 5.1: Trade-off security vs. usability

On the other hand, two of the security experts, Security Expert C and Security Expert A, meant that, in general, more demanding security mechanisms create a hassle for the users, whereby they will find shortcuts to get around the mechanisms. We found that Security Expert A agrees with Nepal, who, as mentioned in Section 2.4 stated that there is not enough focus on usability. Usability above security is great if we do not experience a security incident, and understandably we might want more security mechanisms if we have experienced a social engineering attack. Hence, the challenge here is to find a good trade-off, illustrated in Figure 5.1.

Information Security Awareness

All of the interviewees talked about ISA and they all agreed that it is a useful tool to prevent social engineering attacks. However, it was only the security experts that elaborated about security awareness training. The victims did not say anything further than that they thought it is useful to raise awareness. One of the problems with security awareness training that can cause it to not be as effective it theoretically should be is that the training often is inefficient when it comes to changing people's behavior, as pointed out in the literature, presented in Section 2.3.2. The literature points out that although the employees are aware of how they theoretically should behave, other factors like stress and time make employees not follow what they have learned in the security awareness training. The interviewees also mentioned practical challenges with following security advice, like *we cannot avoid clicking on all links* and that *we could have a bad day*. When the security experts talked about ISA they focused on having awareness training that made the information stick and providing specific and tangible advice that would be helpful for the users, focusing on the difficulty of having security training that fits everyone in an organization. This focus

can be a result of them feeling like security awareness training does not stick, and that employees tend to fade out the training, or maybe they do not learn anything from it, or that stress and other factors get in the way.

As presented in Section 2.3.2 Bulgurcu et.al states the importance of compliance, hence that if employees comply with the security policy they can serve as information security assets. Security Expert A has similar thoughts as Moore who stated that a compliance based security approach is prone to fail, as presented in Section 2.3.2. Security Expert A was not only positive to a compliance driven approach. He meant that the main drive for ISA training needs to be the goal of learning and increasing the employees' knowledge about information security in order to be effective, instead of management only having a goal of checking off the completed training. We believe that in order for people to serve as assets when it comes to security and for the awareness training to be purposeful it is important to motivate security compliance behavior in regards to the organization's security policy. However, we believe the goal for security awareness training should not solely be compliance driven, above all it should be driven by increasing the information security knowledge to those who participate in the training.

Another challenge with ISA training is that it is difficult to make the training efficient against personalized attacks. Security awareness training can give general advice and raise awareness around attacks and countermeasures, but it is hard to even discover attacks when they are very personalized, as seen with the incidents to Victim C, Victim A, Victim D and Victim B. It is difficult to provide training that prepares one for such personalized attacks, especially attacks similar to the ones to Victim C and the crypto scam, as presented in Section 2.1.4.

5.2.2 Attitudes and behavior

Trust as an asset or a challenge

Even though we have security measures and security awareness training we still trust people. Trust is, as commonly known, a central tool in almost all social engineering attacks which can result in that we ignore security training and security policies, and social engineering attacks take advantage of this. From the interviews, we conclude that one of the reasons why trust is so important when it comes to falling for social engineering attacks is because trust is essential for making people help you and doing favors for you. As seen from the interviews, when we trust someone we want to help them, and then we are more prone to not be as skeptical to requests.

Attackers take advantage of this and it can result in huge consequences. The crypto scam NRK published, described in Section 2.1.4, shows how trust made people less skeptical of receiving "help" and then performing actions resulting in financial

loss. In the incident to Victim C, trust and love was some of the main factors as to why the attacker managed to be successful. These examples of industrialized social engineering shows how important trust is.

According to Statistisk Sentralbyrå (SSB), Norwegians are the most trusting citizens in Europe towards political institutions such as the police or politicians [70]. This was an advantage during the Covid-19 pandemic, when the population trusted the government. But trust is not always good because it can be a disadvantage for Norwegians when looking at susceptibility towards social engineering attacks. This level of trust might be a factor why "older ladies" still want to believe that love scams are real, and why Victim C trusted the man that scammed her. It is easier to leverage trusting people. However, trust can be positive in regards to moving on after a social engineering attack. Victim C said that she still trusts people and that she chooses to believe that the incident she was involved in was so special that she cannot stop trusting people just because of what she experienced. Security Expert A said that he do not want to destroy the trust level in Norway, even though he knows that the consequences of trusting the wrong people can be big, because he values the benefits of trust more than the challenges.

However, how much trust we should give people and which precautions to take to protect ourselves is a fine line. We conclude from the interviews that too little trust will negatively impact people's lives, but trusting the wrong people or having too much faith that people take sufficient security precautions can also damage. Trusting that your colleagues have followed the established security policies and precautions can create repercussions, as seen by the incident Victim A was involved in. The colleagues' trust in each other was one of the reasons why the attack succeeded because everyone assumed that the others had quality-checked the fraudulent email. From the interviews, we gather that this shortcoming occurs because not trusting that your colleagues have checked things sufficiently, and doing duplicated work by checking yourself will decrease productivity and create doubt between co-workers, which can contribute to a negative culture within the organization.

Blaming successful attacks on bad luck

From the interviews, we see that almost all of the interviewees did not believe luck or coincidence was the reason why a social engineering attack was successful, in contrast to *Mørketallsundersøkelsen 2020*. This may be because bad luck or coincidence was an option in *Mørketallsundersøkelsen* when the participants were asked which factors they believed caused a security breach. Hence this answer may have seen more correct for the participants than the other answers provided in the survey. This is a contrast to when we asked the interviewees about their thoughts about whether or not they believed luck or coincident was the reason why a social engineering

attack was successful. We also specifically asked about social engineering, whereas *Mørketallsundersøkelsen* asked about security breaches in general.

Security Expert B meant that it can be bad luck that you were targeted or became a goal, but contrary to Security Expert C she does not believe that it is bad luck that you fall for the social engineering attack. Security Expert C stated that he believes that it can be bad luck sometimes because you can be subjected to an attack before it is known, or you can have a bad day for instance. We believe this way of thinking can, as Victim A mentioned, be unwise and a way to not take the blame or make changes or implement countermeasures. As Victim A noted, if we do not give the reason for a successful attack further reflection, it can cause people to believe that humans are the weakest link or blame it on bad luck, which can cause that they do not seek out the actual cause of the problem but attribute it to human weakness.

Security Expert A talked a lot about how we have much to learn from other more traditional industries like aviation and health care. In the aviation industry, for instance, Security Expert A claimed bad luck is not considered a reason why something goes wrong. As Security Expert A implied there is always a reason why something fails or goes wrong and we agree with him and believe that the cyber security field should learn from this and always ask why something happened and not blame it on bad luck or coincident. Why this is not the case in cyber security may be because it is a young field that does not have the same traditions other fields and industries have, but we believe cyber security could learn from this.

Shame cripples transparency

During the interviews, we discovered the importance of shame as an aftereffect of successful social engineering attacks. Shame can come from the victim's thoughts, for example they can feel that they should have realized what was going on. Shame can also originate from other individuals who blame or guilt the victim for falling for the scam. Victim C emphasized that she has encountered several social engineering victims who, like herself, felt shame caused by themselves and how others acted after the attack. Figures 5.2 and 5.3 displays some of the comments people left on social media about Victim C after the incident she was involved in became known. Whether Victim C and other victims are to blame for the position they are in is another discussion, this section merely addresses that comments like the ones displayed can inflict the feeling of shame both for Victim C herself and others who see the negative comments.



Figure 5.2: Negative comments on social media about Victim C's experiences



Figure 5.3: Positive comments on social media about Victim C's experiences

This topic is not something we have seen much of in earlier papers about social engineering, but from what we gather, it is an important element to consider when looking at why existing countermeasures continue to fail. This is because shame reduces the willingness to be transparent. Thus, the advantages described in Section 5.1.2 are lost. The victims might also need more time to recover from the attack if they feel stronger shame, which makes the attack even more costly for the affected parties. As displayed in Section 4.3.3, Victim A and UiT have identified shame and blame as elements they want to avoid in cases like these.

5.2.3 "This will not happen to me"

Security Expert A mentioned, as presented in Section 4.3.1, that he believes that many people think "This will not happen to me". Victim B substantiated this by saying that before the incident happened to him he thought that "this does not happen to me", as presented in Section 4.3.6. Such way of thinking can be destructive and troublesome. It can cause people to not do required measures, because social engineering attacks is something they believe does not relate to them, and therefore it is little need to learn how to protect themselves against such attacks. This can cause that countermeasures against social engineering attacks are not learned or focused on or that they are being ignored.

5.3 RQ3: Challenging the idea of humans as the weakest link

Whether humans are the weakest link within security or not has been discussed for a long time. It is a question without any definitive conclusions, because of the subjective perspectives people use when discussing this. Different perspectives have been presented for several years, and also manifested themselves with the various interviewees.

Among the interviewees, only Victim B fully agreed with the statement. Moreover, he is one of the interviewees with the least digital competence, which could have affected his viewpoint. As for Victim B's viewpoint, he did not elaborate further than to say that he believes people do not pay enough attention. Security Expert E, Victim D and Victim A share to some degree the understanding that humans can be the weakest link. Their arguments differ, but the bottom line is that they believe humans are the weakest link when gaps in the security of the system exists. Security Expert E's reasoning is that because people have to be able to perform their tasks, and in order to do so, some security measures have to be removed, meaning that it is the needs of the users, not their attitudes or general behavior that make humans the weakest link.



Figure 5.4: Cartoon about humans as the weakest link, inspired by [43]

The literature review revealed that the statement humans are the weakest link has often been taken for granted and accepted without further explanation or "proof". Many articles reference other articles that also state that humans are the weakest link, without providing any evidence either. Figure 5.4 illustrates the attitude towards humans in security, where they are seen as the main source of security challenges, as opposed to all the seemingly superior technical solutions. Security Expert A highlighted an interesting take on "Humans as the weakest link," and Sasse and Adams' article [3]. He emphasized that the authors of the article intended their message to emphasize that the user is not the problem when it comes to password security; the problem is the system and how strict policies affect user behavior. Later, however, there have been subsequent arguments that users' flaws prevent strong passwords from being maintained, making them the weakest link.

We believe that whether you regard humans as the weakest link within security or not has great implications when working with matters of social engineering. This is

because the measures you choose to implement and focus on to prevent these attacks rely heavily on how you look at humans in the security chain. Looking at humans as the weakest link might lead to a culture where more blame is placed on the actor that was tricked than if other links are seen as weaker in the security chain. We believe this can lead to more shame when being subjected to a social engineering attack, which again can create negative repercussions like not letting the IT department know right away because of the fear of negative response. Viewing humans as the weakest link can also prevent us from finding the root cause as to why the attack was successful and find out what can be done in the future in order to prevent similar attacks. Viewing humans as the weakest link can result in increased ISA training in order to try to minimize the damage humans can do, but on the same time it can put the focus on creating too demanding policies as a measure to try to minimize human error, or so called misbehavior. This can however, as Security Expert A pointed out increase security fatigue among users because it might seem hopeless to keep striving for optimal security behavior if you consider yourself the weakest link no matter what. The paradox Sasse and Adam presented [3], where increased security mechanisms lead to less secure behavior, seems to still be accurate, 20 years later.

Both Security Expert A and Security Expert C mentioned in the interviews that humans can be used as a security resource, agreeing with Pfleeger and Furnham [61], because we can notice things that machines cannot. Security Expert A emphasized that humans can be utilized a lot more to be a security resource, and we agree with this. Switching the mindset of humans being the weakest link to that humans are a security resource can as seen from the interviews empower users, which can increase users willingness to focus on ISA training and be more aware against social engineering if they know that they are viewed as an asset instead of a security risk.

In general the interviewees have opposing opinions to the question of humans as the weakest link, agreeing and disagreeing with both each other and the presented research. However, the elaborations to their opinions provide valuable nuances to the discussion.

5.4 RQ4: Countermeasures and recommendations against social engineering attacks

This section discusses countermeasures and recommendations mentioned in the interviews as well as those described in the literature as presented in Chapter 2. Further information on the recommendations and countermeasures is provided in the following sections. Lastly, a list of recommendations which we believe to be useful in reducing social engineering attacks is presented to sum up the most important recommendations discussed in the previously sections.

5.4.1 Policies can enforce or weaken the security of a system

As discussed, misaligned incentives and legislation can cause the part that can enforce a countermeasure to choose not to do it. Therefore, we recommend that precise methods to distribute the "question of responsibility" when a party is deceived are established. If this is established beforehand, then each party will have incentives to enforce and implement measures that can protect from unwanted situations and thus help reduce the damage of successful social engineering attacks as well as the number of successful attacks.

As a result of the interviews, we conclude that management and decision makers should have a reflective and conscious approach to policies. As seen from the interviews, we believe that it is essential not to enforce too many policies because it can be overwhelming for the users. This can result in the users ignoring the policies or finding ways around them. Therefore, we recommend having a conscious relationship to risks and which risks the organization is willing to accept. One example of this is that the organization Security Expert E is a part of makes an active choice where they accept the risks of not using name tags. Enforcing policies on the most essential things and regarding other things as best practices can be a way of having a conscious relationship to risks and not overwhelming the employees.

We conclude from the interviews that banks can implement policies that will improve the security to the users related to at least social engineering attacks. Among the policies mentioned by Victim C there can be one in which, when transferring money, the banks impose a limit per transfer that is transferred immediately. Transferring more than this limit freezes the transfer for a time period before it is sent so that the transfer can be changed or canceled. This policy could be the default in the online bank, but users who want to turn it off can do so. Despite this policy's preference for security over usability, users can disable it themselves to decide whether they want it turned on or not. Because of status quo bias, most users will most likely have the default setting on. We believe this policy can help many potential victims of social engineering. Many people will tell someone about the incident after a short time period and later regret their action, so the ability to regret that action could contribute to fewer successful social engineering attacks and financial loss.

Another example of status quo bias being present is related to ISA training. Organizations can enforce standardized ISA training because "everyone is doing this," even though this training is not that effective for the organization. They may have different needs and knowledge that needs to be covered differently. Therefore standardized ISA training may not be the best countermeasure against social engineering for every organization. Therefore we suggest trying to find ISA training that is best suited for the needs of the organization.

5.4.2 Aligning security culture with organizational culture

One of the main recommendations found from the interviews is to align the security culture with the organizational culture, as discussed in Section 5.1.2. This is important to get employees along on the security team and make security a part of the culture rather than being something regarded as troublesome, that crash with the established routines and hinder work efficiency. Consequently, it is necessary that the security policies become an interwoven part of the organizational culture.

5.4.3 Technical measures

The interviewees and literature recommended several technical measures that protect against social engineering attacks, as presented in Sections 4.5.2 and 2.3.2. Regardless of whether humans are considered the weakest link or not, it is clear that technical measures such as email filters are relevant to protecting users from phishing attacks, for example. From the interviews, we gathered that technical measures that make users feel like it is easy to act securely are valuable. One such tool is an add-on that can be implemented in the email service that the users can use to indicate that an email they receive seems suspicious, thus making them an active part of the email filter.

In USA there exists a service where "ordinary" people can anonymously share fraudulent attempts with each other based on location and type of scam [71], as seen in Figure 5.5. This type of crowd-sourcing can be used by the users to warn each other of different scams and spread knowledge and increase transparency. Such a service does not exist in Norway, but we believe this could be a good measure against social engineering attacks. Moreover, such warnings and knowledge is not limited to closed forums; the service is open to everyone. With the service being anonymous, it can decrease the threshold for posting, making more people share incidents of attacks. However, some limitations with such a service are quality control because everyone can share knowledge and warnings. Furthermore, even though those who post are anonymous, they can experience that their story is being shamed, which can make them feel stupid and blamed for posting, hence scaring them and others away from warning about future incidents.

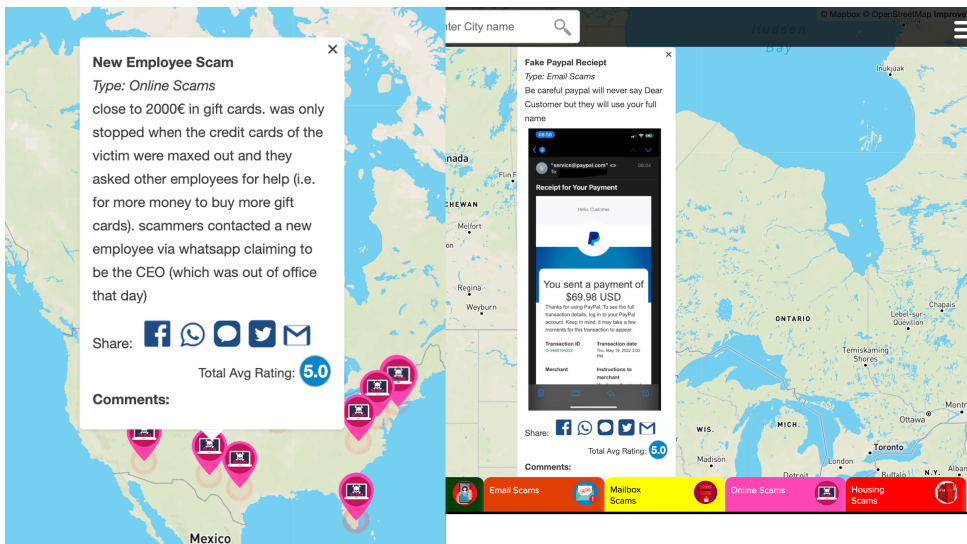


Figure 5.5: Sharing scams [71]

5.4.4 Attitude change as a defense mechanism

Our recommendations against social engineering attacks include changes in attitude. The media has started to pick up on cases relating attitude changes with blaming victims of social engineering, especially related to Victim C and other investment scams [73, 74]. However, we have not seen this theme brought up too much in literature regarding social engineering, so we want to shed light on this and get it on the agenda.

This attitude change includes the perception that humans are the weakest link in a security chain. Unfortunately, during the interviews, it was clear that this statement still has a foothold, which is also observed in articles, as mentioned in Section 2.4. For example, Victim B stated that humans are inattentive and that this is one of the reasons we are the weakest link, and it is easy to blame it on matters like this or other reasons like we are too lazy and that we make mistakes.

Stating that humans are the weakest link and protecting it with arguments like this prevents us from finding the root cause of why a social engineering attack was successful. Furthermore, by not finding the root cause it is difficult to learn from the incident and find ways to prevent the same thing from happening again. The same is true for blaming successfully social engineering attacks on luck or coincident, therefore we recommend to stop blaming successful attacks on luck, coincident or humans being the weakest link, and start to ask the question why until we disclose the reason

why the attack was successful. This is not to say that we should not acknowledge weak human behavior, but instead of only blaming people to be inattentive for instance, we should rather focus on how to increase awareness. In Section 5.3, we described how we believe it would be beneficial to switch the mindset from seeing humans as the weakest link to seeing them as a security resource, as illustrated in Figure 5.6. We believe that such a change of attitude can reduce successful engineering attacks because it can empower and motivate people to pay more attention to social engineering attacks if they know they can be of assistance.

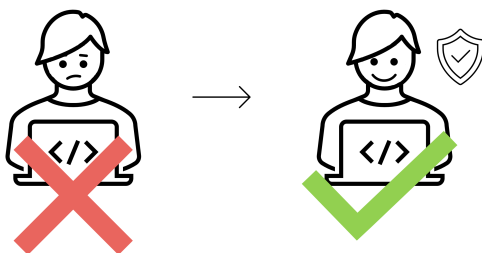


Figure 5.6: Illustration about switching perception from humans as the weakest link to humans as a security resource

In line with this empowerment, we want to introduce a new concept, namely *Security 2*, which focuses on the many things that go well instead of only looking at the things that go badly. In reviewing this thesis, we felt that too much focus was placed on which countermeasures and behavior need to be improved to stop social engineering attacks as well as much attention on the social engineering attacks that succeed, but little on those we have stopped. A way to empower people and give them digital confidence can be to tell stories where someone has been able to prevent a social engineering attack and explain how they did this. By sharing stories of social engineering attacks we have prevented and detected, we believe new recommendations on how we can improve security can be developed and shared. Additionally, we believe that this will give people a sense of motivation, making them more inclined to focus on preventing social engineering attacks when they know it is possible.

The inspiration for naming this concept *Security 2* comes from the known concept *Safety 2*. Safety 2 is a concept that was introduced as a contrast to the original and traditional safety term, often called Safety 1 [41]. Safety 1 focuses on everything that can go wrong and assumes that the error is because of malfunctions or failures that can be identified, where factors contributing to such failures are usually identified as technological, human, or organizational factors. In contrast, Safety 2 focuses on the capability of the organization to succeed under varying conditions and emphasizes

that more things go well than wrong. According to Hollnagel et al. [41], the Safety 1 approach, focusing on everything that goes wrong, does not indicate what can be done to improve safety. We believe that this also applies to security, not only social engineering but also to the entire cyber security domain. We believe that *Security 2* is a concept that can be useful in fighting social engineering attacks, and we recommend that it will be further researched.

Another attitude change we believe is important is to remove the shame related to being a victim of a social engineering attack. As discussed previously, shame can negatively affect the security because it can lead to less transparency relating attacks. In order to reduce this feeling of shame we believe that one initiative is to discuss and be open about social engineering incidents when they occur, as well as meeting victims with respect instead of blame, and focus on how it can be prevented in the future. Findings from the interviews show that some organizations already focus on reducing the shame connected to falling for social engineering, as stated by Victim A and Security Expert D in Section 4.3.3, implying that shame is on the agenda for some organizations already. Security Expert A also said that reduced shame can increase trust within an organization. Hence another benefit of reducing shame is that the damage made by social engineering attacks can, in some cases, be dealt with quicker because the victim alerts relevant actors earlier when they are not afraid of being shamed for their mistake.

5.4.5 List of recommendations

Even though we provide a set of recommendations to reduce successful social engineering attacks, it is not our intention to give recommendations that you can check off and then move on. Instead, we believe that the security culture should be aligned with the organizational culture, and focus should be placed on countermeasures that involve information security in the everyday choices for an individual or organization. The following list presents the most essential recommendations that are based on the findings in this study. The recommendations are ideas to ways of thinking, more than explicit "to-dos".

- *Security 2*: focus on everything that works to prevent attacks, not only what fails
- Change the perception that humans are the weakest link to that humans are a security resource
- Stop blaming successful social engineering attacks on luck or coincidence
- Be transparent about security incidents, both as organizations and individuals
- Reduce the shame related to being a victim of a social engineering attack

- Avoid a compliance-based approach to security as the main security approach
- Align and interweave the security culture with the organizational culture
- Identify incentives to implement and invest in security measures and align responsibilities accordingly
- Management and decision-makers should have a reflected and conscious approach to policies and which risks they are willing to accept, enforcing policies on what is most important and regard other policies as "best practice"
- Use a side channel for confirmation whenever a party wants to alter information that can cause significant damage if the new information is crooked, such as payment details
- Implement an add-on in email services where users can report suspicious emails
- Create an open platform for people to share security incidents anonymously

5.5 Threats to validity

The project is based on information gathering from semi-structured interviews, where the focus was to get the interviewees talking, without interrupting them too much. As a result not all questions were asked to all interviewees, because they either covered the topic before the question was proposed, or the question was deemed less relevant for the current interviewee. Having different questions, and thus answers, to evaluate for the various interviewees makes comparisons across interviews harder.

Another challenge we discovered in some interviews that affected our results is the language barrier between the interviewees, who speak Norwegian, and the terminology within security economics and other fields, where English is used. The security economics terminology was also rather unknown for interviewees. As a result, several of the interviewees were unfamiliar with concepts within security economics, which made it more challenging to ask questions directly about how security economics could be applied to the relevant case. This led to the need for examples to illustrate the topics to avoid confusion. However, there is a risk that the specific intention of some questions is lost when relying on examples to explain.

Furthermore, the interviewees can only describe their own experiences. Particularly with the victims of social engineering attacks, their personal feelings color their experiences and descriptions of what happened and how other actors met them. Therefore, a limitation to this project is that we only have presented one side of each case. We do not know how the other actor involved in Victim B and Victim A's cases look at the situation, and with regards to the actors that Victim C criticizes, we only

have their official statements available in newspapers to indicate how they feel about Victim C's statements. Therefore, it is likely that our discussion is somewhat biased by the interviewees' perspectives, even though this is something we are aware of and try to minimize.

Chapter 6

Conclusion and Future work

In this thesis, we have gathered data from victims of social engineering attacks and information security experts and explored how existing theories within security economics coincide with our data. To a large extent, our findings substantiate the established theories and contribute to the existing literature by shedding light on how concepts from security economics can improve our understanding of why social engineering attacks succeed. The project has been guided by four research questions, looking both at theoretical and empirical data and concepts. The empirical data comes from a qualitative study with semi-structured interviews with various relevant actors, four victims of spoofing, BEC or other social engineering attacks, and five security experts within different organizations.

Most of the interviewees shared a common understanding of why social engineering attacks are successful, which aligns with the existing literature, through exploiting that the victims do not always have sufficient information or do not have the time, resources, or possibility to defend themselves properly. *Culture, trust, shame* and *transparency* were to a large extent pointed at as the most important factors to explain the continued success of the attacks. We believe that these concepts should be added to the research of security economics. This suggests that an interdisciplinary approach is particularly valuable when studying social engineering since these concepts are rarely discussed in technical papers about information security, yet they remain relevant when examining why systems fail. We also found that the actors who can implement measures against social engineering attacks need to have incentives to do so. For instance, banks might need incentives if they should make it more difficult for users to get consumer loans.

This thesis also explored whether or not humans should be seen as the weakest link when it comes to security and why this is a prevailing thought among the population by comparing the perspectives of the various interviewees with each other and relevant literature. In essence, we conclude that defining humans as the weakest link might weaken the overall security because this notion can prevent us from seeing

other weaknesses and hinder identifying why an attack was successful. Therefore, we believe an attitude switch from humans being the weakest link to that humans are security resources are necessary. Furthermore, we believe that another attitude change that will reduce successful attacks and make existing measures work better in reality is to not blame successful social engineering attacks on bad luck or coincidence. Additionally, we believe that showing that social engineering attacks can happen to anyone, from security experts to old ladies. We need to shift the idea people have *from* thinking that “this will never happen to me” or that “everyone who falls for social engineering attacks are stupid”, *to* thinking that attackers can fool anybody.

Based on the interview findings and existing literature, we have presented a selection of suggested recommendations that can reduce the rate of successful social engineering attacks. A central concept here and one of our main findings is to focus on creating a strong security culture that aligns and interweaves in the organization. Countermeasures against attacks should not simply be a list that decision-makers can tick off, such as enforcing three hours of e-learning to all employees. It should be continuous work that is a part of everyone’s mindset, from users to management. Moreover, we believe that it is important to establish a mindset where it is not shameful to fall for scams like this. Policies should not be too demanding and cause *security fatigue*, but rather focus on the most important things. Security 2 is a new concept we suggest as a measure to empower people and give them digital confidence, making people more motivated to fight against social engineering.

6.1 Future Work

To the best of our knowledge Security 2 is not an established concept in the existing literature, but we advocate working further to incorporate it in future literature. We believe Security 2 could be an effective measure in the battle against social engineering, as well as other security challenges and attacks. We urge future researchers to look more into this topic and gather inspiration and insight from *Safety 2*.

Seeing social engineering from a security economics context is not something that has been done empirically before, at least in the literature we have researched. We have looked into several topics related to this that we uncovered in the data gathering, but we believe that more research is needed on the topics covered in this thesis. For instance, we endorse research on how to increase transparency around social engineering attacks and which incentives can motivate different actors to increase transparency. We also believe that other concepts from security economics can also apply to social engineering and would benefit from being researched further.

Reducing shame related to being a victim of social engineering attacks is an important finding we inquire further research on, particularly how to achieve it in

practice. Nevertheless, tackling this problem is tricky; it requires a change of attitude in the population, in addition to educating the public about the fact that “it is not only stupid people” who fall for such scams.

References

- [1] Finansavtaleloven, § 35 - misbruk av konto og betalingsinstrument. <https://lovdata.no/lov/1999-06-25-46>, 2009. (Accessed on 06/06/2022).
- [2] SpareBank 1. Svindelforsøk på e-post (phishing). (Accessed on 11/02/2022). URL: <https://www.sparebank1.no/nb/bank/privat/info/svindel-epost.html>.
- [3] Anne Adams and Martina Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.
- [4] David Airehrou, Nisha Vasudevan Nair, and Samaneh Madanian. Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model. *Information (Basel)*, 9(5):110, 2018.
- [5] George A. Akerlof. The market for “lemons”: Quality uncertainty and the market mechanism. *The Quarterly journal of economics*, 84(3):488–500, 1970.
- [6] Rana Alabdan. Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, 12(10), 2020. URL: <https://www.mdpi.com/1999-5903/12/10/168>, doi:10.3390/fi12100168.
- [7] Hussain Aldawood and Geoffrey Skinner. Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pages 62–68, 2018. doi:10.1109/TALE.2018.8615162.
- [8] Ross Anderson. Why information security is hard - an economic perspective. *Seventeenth Annual Computer Security Applications Conference, IEEE*, pages 358–365, December 2001. doi:10.1109/ACSAC.2001.991552.
- [9] Ross Anderson and Tyler Moore. Information security economics – and beyond. In *Advances in Cryptology - CRYPTO 2007*, Lecture Notes in Computer Science, pages 68–91. Springer Berlin Heidelberg, Berlin, Heidelberg.
- [10] Ross Anderson and Tyler Moore. The economics of information security. *Science*, 314:610–613, 2006.
- [11] Erik Angner. A course in behavioral economics, 2016.

- [12] Michelle Catherine Baddeley. Information security: Lessons from behavioural economics. *In proceedings of Security and Human Behavior 2011*, 2011.
- [13] Devon Baranek and Kathleen M. Bakarich. Something phish-y is going on here: A teaching case on business email compromise. *American Accounting Association*, 14, 2020.
- [14] Johannes M. Bauer and Michel J.G. van Eeten. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10):706–719, 2009. URL: <https://www.sciencedirect.com/science/article/pii/S0308596109000986>, doi:<https://doi.org/10.1016/j.telpol.2009.09.001>.
- [15] Susan E. Beck and Kate Manuel. *Practical research methods for librarians and information professionals*. Neal-Schuman Publishers, 2008.
- [16] Preben Brækstad. Når noen ringer fra banken, er det lett å tro på det. (Accessed on 31/01/2022). URL: <https://www.adressa.no/pluss/nyheter/2022/01/31/N%C3%A5r-noen-ringer-fra-banken-er-det-lett-%C3%A5-tro-p%C3%A5-det-25026052.ece>.
- [17] Roderic Broadhurst. Developments in the global law enforcement of cyber-crime. *Policing : an international journal of police strategies management*, 29(3):408–433, 2006.
- [18] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34:523–548, 2010.
- [19] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3):523–548, 2010.
- [20] Rainer Böhme and Galina Schwartz. Modeling cyber-insurance: Towards a unifying framework. *The Ninth Workshop on the Economics of Information Security (WEIS 2010)*, 2010.
- [21] National Cyber Security Center. Phishing attacks: defending your organisation. (Accessed on 08/02/2022). URL: <https://www.ncsc.gov.uk/guidance/phishing>.
- [22] Carlos Perez Chalico. Your employees are the weakest link in your cybersecurity chain. (Accessed on 10/05/2022). URL: https://www.ey.com/en_ca/cybersecurity/your-employees-are-the-weakest-link-in-your-cybersecurity-chain.
- [23] David Coghlan and Mary Brydon-Miller. *The SAGE Encyclopedia of Action Research*, volume 2. London: SAGE Publications, 2014. URL: <https://methods.sagepub.com/reference/encyclopedia-of-action-research/n273.xml>, doi:10.4135/9781446294406.
- [24] Adéle da Veiga, Liudmila V Astakhova, Adéle Botha, and Marlien Herselman. Defining organisational information security culture—perspectives from academia and industry. *Computers and security*, 92:101713–23, 2020.

- [25] Adéle da Veiga and Nico Martins. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and security*, 49:162–176, 2015.
- [26] Dagbladet. Ikke klikk på lenken. (Accessed on 31/01/2022). URL: <https://dinside.dagbladet.no/mobil/ikke-klikk-pa-lenken/74418600>.
- [27] Elaine Denny and Annalise Weckesser. Qualitative research: what it is and what it is not. *England: Wiley Subscription Services, Inc*, 126:369, 2019. doi: 10.1111/1471-0528.15198.
- [28] Milena Dinkovay, Ramy El-Dardiry, and Bastiaan Overvesty. Cyber incidents, security measures and financial returns: Empirical evidence from dutch firms. *The 2020 Workshop on Economics and Information Security (WEIS)*, 2020.
- [29] e24. Dnb utsatt for massive phishing-angrep. URL: <https://e24.no/naeringsliv/i/1OW3PK/dnb-utsatt-for-massive-phishing-angrep>.
- [30] e24. Nytt phishing-angrep ved offentlig petroleumsinstitusjon. (Accessed on 31/01/2022). URL: <https://e24.no/teknologi/i/K3OEe5/nytt-phishing-angrep-ved-offentlig-petroleumsinstitusjon>.
- [31] DNB Financial Cyber Crime Center (FC3). Annual fraud report 2021. *DNB*, 2021.
- [32] Ana Ferreira, Lynne Coventry, and Gabriele Lenzini. Principles of persuasion in social engineering and their use in phishing. In *Human Aspects of Information Security, Privacy, and Trust*, pages 36–47. Springer International Publishing, 2015.
- [33] Anders Lohne Fosse. Ny hackingmetode sprer seg fort: – veldig omfattende. <https://www.nettavisen.no/nyheter/ny-hackingmetode-sprer-seg-fort-veldig-omfattende/s/12-95-3424187943>, 10 2021. (Accessed on 05/28/2022).
- [34] John Gray. *An Efficient Remedy for the Distress of Nations*. 1842.
- [35] Philip Haglund and Julie Solberg. Ble kontaktet av internasjonal superstjerne etter datahacking: Tipset fikk en hel verden til å sperre opp øynene. <https://www.nettavisen.no/livsstil/ble-kontaktet-av-internasjonal-superstjerne-etter-datahacking-tipset-fikk-en-hel-verden-til-a-sperre-opp-oynene/s/12-95-3424243282>, 02 2022. (Accessed on 05/28/2022).
- [36] T Harbert. The weakest link in cybersecurity. (Accessed on 11/05/2022). URL: <https://www.shrm.org/hr-today/news/all-things-work/pages/the-weakest-link-in-cybersecurity.aspx>.
- [37] Joseph M Hatfield. Social engineering in cybersecurity: The evolution of a concept. *Computers and security*, 73:102–113, 2018.

- [38] Ryan Heartfield and George Loukas. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Comput. Surv.*, 48(3), dec 2015. doi:10.1145/2835375.
- [39] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. *Proceedings of the 2009 workshop on Newsecurity paradigms workshop*, pages 133–144, 2009.
- [40] Jonas Hielscher, Annette Kluge, Uta Menges, and M. Angela Sasse. "taking out the trash": Why security behavior change requires intentional forgetting. *Association for Computing Machinery*, page 108–122, 2021. doi:10.1145/3498891.3498902.
- [41] E. Hollnagel, R.L. Wears, and J Braithwaite. From safety-i to safety-ii: A white paper. 2015. URL: <https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-white-papr.pdf>.
- [42] Hang Hu and Gang Wang. Revisiting email spoofing attacks, 2018. URL: <https://arxiv.org/abs/1801.00853>, doi:10.48550/ARXIV.1801.00853.
- [43] j klossner cartoons. Technology cartoons — j klossner cartoons. <http://www.jklossner.com/humannature>. (Accessed on 06/04/2022).
- [44] Markus Jakobsson. *Understanding Social Engineering Based Scams*. Springer New York, New York, NY, 2016.
- [45] Nicola Jentzsch. State-of-the-art of the economics of cyber-security and privacy. *IPACSO Deliverable D*, 4, 2016.
- [46] Odin Johannessen. Mørketallsundersøkelsen 2020. (Accessed on 10/05/2022). URL: <https://www.nsr-org.no/aktuelt/m%C3%B8rketallsunders%C3%B8kelsen-2020>.
- [47] Kommune-CSIRT. Digitalt situasjonsbilde. Rapport nr. 2 - 2021:1–10, 2021.
- [48] K. Krombholz, H. Hobel, M. Huber, and E Weippl. Advanced social engineering attacks. : *Journal of Information Security and Applications*, pages 113–122, 2015.
- [49] Benedikt Lebek, Jörg Uffen, Michael H. Breitner, Markus Neumann, and Bernd Hohler. Employees' information security awareness and behavior: A literature review. In *2013 46th Hawaii International Conference on System Sciences*, pages 2978–2987, 2013. doi:10.1109/HICSS.2013.192.
- [50] Mai Scott Linneberg and Steffen Korsgaard. Coding qualitative data: a synthesis guiding the novice. *Qualitative Research Journal*, 19:259–270, 2019. doi:10.1111/1471-0528.15198.
- [51] Graham Mallard. *Behavioural economics*. Economy, key ideas. Agenda Publishing, Newcastle upon Tyne City, 2017.

- [52] Vilde Kristine Malmo, Rune N. Anreassen, and Inghild Eriksen. Uit svindlet for 12 millioner. (Accessed on 23/03/2022). URL: <https://www.nrk.no/tromsogfinnmark/et-av-norges-storste-universitet-svindlet-for-12-millioner-1.14830758>.
- [53] Per Håkon Meland. Storyless cyber security: Modelling threats with economic incentives, 2021. URL: <https://hdl.handle.net/11250/2825312>.
- [54] Tyler Moore. The economics of cyber-security: Principles and policy options. In *In Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, chapter 1, pages 3–24. The National Academies Press, Washington, DC, 2010.
- [55] Tyler Moore. The economics of cybersecurity: Principles and policy options. *International journal of critical infrastructure protection*, 3(3):103–117, 2010.
- [56] Tyler Moore, Richard Clayton, and Ross Anderson. The economics of online crime. *The Journal of economic perspectives*, 23(3):3–20, 2009.
- [57] Felicity Morris and Bernadette Higgins. *The Tinder Swindler*. Netflix, feb 2022.
- [58] Surya Nepal. Security is the weakest link: Prevalent culture of victim blaming in cyberattacks. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, Asia CCS '19, page 255–256, New York, NY, USA, 2019. Association for Computing Machinery. doi : 10.1145/3321705.3329914.
- [59] Nettavisen. Betalte 3000 kroner for en mobiltelefon han aldri fikk: - folk er for godtroende. <https://www.nettavisen.no/nyheter/innenriks/betalte-3000-kroner-for-en-mobiltelefon-han-aldri-fikk-folk-er-for-godtroende/s/12-95-3423413669>, 2018. (Accessed on 05/28/2022).
- [60] S. Oriot, A. Williams, and J Dykstra. Omnichannel Cybersecurity: Optimizing Security by Leveraging Asymmetric Motivation. *The 20th Annual Workshop on the Economics of Information Security (WEIS 2021)*, 2021. URL: <https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-oriot.pdf>.
- [61] Shari Lawrence Pfleeger, M. Angela Sasse, and Adrian Furnham. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, 11(4):489–510, 2014. URL: <https://doi.org/10.1515/jhsem-2014-0035> [cited 2022-05-11], doi :doi:10.1515/jhsem-2014-0035.
- [62] Secure Practice. Security with a human touch. (Accessed on 23/03/2022). URL: <https://securepractice.co/about>.
- [63] PurpleSec. 2021 cyber security statistics: The ultimate list of stats, data & trends. <https://purplesec.us/resources/cyber-security-statistics/>, 2020. (Accessed on 05/11/2022).
- [64] Ken Pyzik. Shutting the door on social engineering. *Internal Auditor*, 72 (5):20–21, 2015.

- [65] Bruce Schneier. Semantic attacks: The third wave of network attacks. (Accessed on 07/02/2022). URL: <https://www.schneier.com/crypto-gram/archives/2000/1015.html#1>.
- [66] Alexander Schulan. Behavioural economics of security. *European journal for security research*, 4(2):273–286, 2019.
- [67] Shatadru Shikta, Somania Nur Mahal, Kazi Bushra Al Jannat, Mahady Hasan, and M. Rokonzaman. Behavioral economics issues for software requirements optimization for personal data security and privacy. *2021 7th International Conference on Computer Technology Applications*, pages 38–45, 2021.
- [68] Sikkerhetsfestivalen. Silje berg og tilde thorvik — sikkerhetsfestivalen. <https://sikkerhetsfestivalen.no/bidrag2022/silje-berg-tilde-thorvik>, 2022. (Accessed on 05/26/2022).
- [69] Mrinalini Singh and Shivam Singh. Cyber crime convention and trans border criminality. *Masaryk University Journal of Law and Technology*, 1(1):53–66, 2007.
- [70] SSB. Nordmenn på tillitstoppen i europa - ssb. <https://www.ssb.no/kultur-og-fritid/artikler-og-publikasjoner/nordmenn-pa-tillitstoppen-i-europa>, 2016. (Accessed on 05/18/2022).
- [71] Swipealert. Swipe alert - uncover local scams before it affects you. <https://swipealert.co/#>, 2019. (Accessed on 05/26/2022).
- [72] Telenor.no. Hva er spoofing? <https://www.telenor.no/sikkerhet/faq/hva-er-spoofing/>, 2022. (Accessed on 05/27/2022).
- [73] Markus Thonhaugen. Tapte over 7 millioner i svindel, politiet henla på dagen: – drøyt og jævlig. (Accessed on 23/05/2022). URL: https://www.nrk.no/nordland/tapte-over-7-millioener-i-svindell-politiet-henla-pa-dagen-_-_-droyt-og-jaevlig-1.15972132.
- [74] Markus Thonhaugen and Hanne Wilhelms. Kryptosvindelen, 2022. (Accessed on 05/28/2022). URL: https://www.nrk.no/nordland/xl/kryptosvindell-mann-ble-lurt-for-200.000-kroner_-men-folk-svindles-for-millioener-1.15846412.
- [75] Aksel Tjora. *Kvalitative forskningsmetoder i praksis. 3. utgave*. Gyldendal, 2017.
- [76] NRK TV. Dagsnytt 18 - tv – 18. mars – dagsnytt 18 – nrk tv. <https://tv.nrk.no/serie/dagsnytt-atten-tv/202203/NNFA56031822/avspiller>, 2022. (Accessed on 05/30/2022).
- [77] UiT. Uit Norges arktiske universitet. <https://uit.no/finnplassendininord>. (Accessed on 05/25/2022).
- [78] Verizon. Dbir 2021 data breach investigations report. *Verizon*, 2021. URL: <https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf>.

- [79] Verizon. 2022 data breach investigation report (dbir) | verizon. <https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf>, 2022. (Accessed on 05/27/2022).
- [80] Amy Hetro Washo. An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, 4:100126, 2021. URL: <https://www.sciencedirect.com/science/article/pii/S2451958821000749>, doi:<https://doi.org/10.1016/j.chbr.2021.100126>.
- [81] Virginia Wilson. Research methods: Interviews. *Evidence Based Library and Information Practice*, pages 96–98, 2012. doi:[10.18438/B89P5B](https://doi.org/10.18438/B89P5B).
- [82] Affan Yasin, Rubia Fatima, Lin Liu, Awaid Yasin, and Jianmin Wang. Contemplating social engineering studies and attack scenarios: A review study. *SECURITY AND PRIVACY*, 2(4):e73, 2019. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.73>, arXiv:<https://onlinelibrary.wiley.com/doi/pdf/10.1002/spy2.73>, doi:<https://doi.org/10.1002/spy2.73>.
- [83] Gavriela Zeller and Matthias Scherer. A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*, 2020. doi:<https://doi.org/10.1007/s13385-021-00290-1>.
- [84] Zuopeng (Justin) Zhang, Wu He, Wenzhuo Li, and M’Hammed Abdous. Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial management + data systems*, 121(3):613–636, 2021.

Appendix

Information to participating security experts

The following document was sent to the social engineering security experts prior to their participation. The document is written in Norwegian, and approved by NSD.

Vil du delta i forskningsprosjektet

”Social engineering attacks in the light of security economics”?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å samle inn data knyttet til sosial manipulasjon-angrep og sikkerhetsøkonomi, med mål om å bruke innsikt fra dette til å bedre forstå hvordan sosial manipulasjon lykkes som angrep, og hva man kan gjøre for å dempe faren for at slike angrep er suksessfulle. I dette skrevet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Formålet med dette prosjektet er å hente inn data og innsikt fra representanter som jobber i informasjonssikkerhet-industrien, vedrørende fagfeltene sosial manipulasjon (social engineering), sikkerhetsøkonomi (security economics), og generell informasjonssikkerhet. Formålet er å innhente empiriske data fra hendelser, samt statistikk og andre former for data som kan bidra til bedre forståelse av trender innenfor fagfeltet. Sikkerhetsøkonomi tar for seg hvordan man kan bruke begreper og teori fra økonomisk teori for å forstå informasjonssikkerhet, angrep og tiltak bedre. Sosial manipulasjon handler om at en angriper bruker psykologisk manipulasjon for å få tak i sensitiv informasjon eller få et offer til å utføre en uønsket handling. Problemstillingen i dette prosjektet baserer seg på at det ikke er forsket spesielt mye på hvordan teorier fra sikkerhetsøkonomi kan bidra til forståelsen av sosial manipulasjon. Forskningsspørsmålene i oppgaven tar derfor for seg hvordan teori fra sikkerhetsøkonomi kan bidra til økt forståelse av sosial manipulasjon, og hvordan data fra hendelser som involverer sosial manipulasjon kan bidra til å styrke eller modifisere eksisterende teorier innenfor sikkerhetsøkonomi. Basert på funnene ønsker vi også å nysensere tankegangen om at menneske er det svakeste leddet i et sikkerhetssystem.

Ønsket er å bruke datagrunnlaget til å trekke ut noen generaliserte funn og trender som kan brukes for å bedre forstå fenomenet sosial manipulasjon, hvorfor slike angrep lykkes, og å foreslå skadebegrensende grep som kan bidra til at færre slike angrep lykkes i fremtiden.

Prosjektet er en del av masterstudiet ved NTNU, og kommer ikke til å brukes til andre formål enn å fullføre masteroppgaven.

Hvem er ansvarlig for forskningsprosjektet?

Maria Bartnes ved Institutt for informasjons- og kommunikasjonsteknologi ved NTNU er ansvarlig for prosjektet. Per Håkon Meland ved Sintef er veileder, men prosjektet utføres for NTNU, og har ikke noe ytterligere å gjøre med Sintef. Prosjektet utføres av Silje Berg og Tilde Thorvik, som med dette prosjektet fullfører sin mastergrad ved NTNU.

Hvorfor får du spørsmål om å delta?

Vi har bedt deg om å delta grunnet den innsikten du har opparbeidet deg ved å jobbe i sikkerhetsindustrien. Prosjektet vårt avhenger av detaljer fra spesifikke angrep, og data som kan bidra til innsikt i trender, holdninger og kultur i arbeidslivet generelt og sikkerhetsindustrien spesielt, og det er sistnevnte punkt her som gjør at vi mener at det har stor verdi at du deltar i dette forskningsprosjektet.

Beskriv hvordan utvalget er trukket (populasjon, utvalgsriterier og gjerne hvor mange som får henvendelsen), slik at det fremgår hvorfor du spør personen om å delta.

Hvis aktuelt, fortell om du har fått personens kontaktopplysninger fra andre (og hvilke tillatelser du har innhentet for det), eller om andre har sendt ut informasjonen for deg.

Hva innebærer det for deg å delta?

Deltakelse innebærer at vi ønsker å utføre et eller flere intervjuer med deg, der lydopptak av intervjuet vil lagres. Intervjuet kommer til å bestå av et utvalg spørsmål knyttet til sikkerhetsangrep, med fokus på sosial manipulasjon, hvorfor slike angrep utføres, lykkes og forhindres i dag. Det vil også innebære enkelte spørsmål som tar for seg begreper fra sikkerhetsøkonomi, som asymmetrisk informasjon og feiltilpassede incentiver.

Det er frivillig å delta

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

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrevet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

De som vil ha tilgang til opplysningene du oppgir vil være Maria Bartnes og Per Håkon Meland, veiledere fra NTNU, samt Silje Berg og Tilde Thorvik, som skriver den aktuelle masteroppgaven. Navnet ditt og annen personlig informasjon vil enten fjernes eller erstattes i presentasjonen av datagrunnlaget. Ved erstatning av personlig informasjon vil vi erstatte den personlige informasjonen med en kode som lagres på en egen liste adskilt fra øvrige data. Vi følger NTNUs retningslinjer for lagring av forskningsdata, og derfor vil datamaterialet lagres på NTNUs servere. Du som deltaker vil ikke kunne gjenkjennes i publikasjonen vår, med mindre dette er strengt nødvendig og vi inngår en enighet om dette på et senere tidspunkt. Dette har du naturligvis full bestemmelsesrett over selv.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er i midten av juni. Etter prosjektslutt vil personopplysninger og lydopptak fra intervju slettes

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

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

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

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

- NTNU ved Maria Bartnes (maria.bartnes@sintef.no), veileder for prosjektet, eller studentene Tilde Thorvik (tildegt@stud.ntnu.no) og Silje Berg (silber@stud.ntnu.no).

- Vårt personvernombud: Thomas Helgesen (epost: thomas.helgesen@ntnu.no, telefon: 930 79 038)

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

- Personverntjenester på epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Maria Bartnes
(Forsker/veileder)

Tilde Thorvik
(Student)

Silje Berg
(Student)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Social engineering attacks in the light of security economics*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i *intervju*
- at opplysninger om meg publiseres slik at jeg kan gjenkjennes [beskriv nærmere] – hvis dette blir aktuelt*

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

(Signert av prosjektdeltaker, dato)

Appendix **B**

Information to participating victims

The following document was sent to the social engineering victims prior to their participation. The document is written in Norwegian, and approved by NSD.

Vil du delta i forskningsprosjektet

”Social engineering attacks in the light of security economics”?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å samle inn data knyttet til tilfeller der sosial manipulasjon-angrep har funnet sted. Målet er å bruke innsikt fra dette til å bedre forstå hvordan sosial manipulasjon lykkes som angrep, og hva man kan gjøre for å dempe faren for at slike angrep er suksessfulle. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Formålet med dette prosjektet er å hente inn data og innsikt fra representanter som jobber i informasjonssikkerhet-industrien, vedrørende fagfeltene sosial manipulasjon (social engineering), sikkerhetsøkonomi (security economics), og generell informasjonssikkerhet. Videre er formålet er å innhente empiriske data fra hendelser der sosial manipulasjon har vært brukt på en suksessfull måte, samt statistikk og andre former for data som kan bidra til bedre forståelse av trender og mekanismer innenfor fagfeltet.

Sikkerhetsøkonomi tar for seg hvordan man kan bruke begreper og teori fra økonomisk teori for å forstå informasjonssikkerhet, angrep og tiltak bedre. Sosial manipulasjon handler om at en angriper bruker psykologisk manipulasjon for å få tak i sensitiv informasjon eller få et offer til å utføre en uønsket handling. Problemstillingen i dette prosjektet baserer seg på at det ikke er forsket spesielt mye på hvordan teorier fra sikkerhetsøkonomi kan bidra til forståelsen av sosial manipulasjon. Forskningsspørsmålene i oppgaven tar derfor for seg hvordan teori fra sikkerhetsøkonomi kan bidra til økt forståelse av sosial manipulasjon, og hvordan data fra hendelser som involverer sosial manipulasjon kan bidra til å styrke eller modifisere eksisterende teorier innenfor sikkerhetsøkonomi. Basert på funnene ønsker vi også å nyansere tankegangen om at menneske er det svakeste leddet i et sikkerhetssystem.

Ønsket er å bruke datagrunnlaget til å trekke ut noen generaliserte funn og trender som kan brukes for å bedre forstå fenomenet sosial manipulasjon, hvorfor slike angrep lykkes, og å foreslå skadebegrensende grep som kan bidra til at færre slike angrep lykkes i fremtiden.

Prosjektet er en del av masterstudiet ved NTNU, og kommer ikke til å brukes til andre formål enn å fullføre masteroppgaven.

Hvem er ansvarlig for forskningsprosjektet?

Maria Bartnes ved Institutt for informasjons- og kommunikasjonsteknologi ved NTNU er ansvarlig for prosjektet. Per Håkon Meland ved Sintef er veileder, men prosjektet utføres for NTNU, og har ikke noe ytterligere å gjøre med Sintef. Prosjektet utføres av Silje Berg og Tilde Thorvik, som med dette prosjektet fullfører sin mastergrad ved NTNU.

Hvorfor får du spørsmål om å delta?

Vi har bedt deg om å delta på grunn av et sikkerhetsangrep du har vært utsatt for, som går under kategorien sosial manipulasjon. Prosjektet vårt er avhengig av å hente inn erfaringer fra virkeligheten, og at vi får detaljer fra prosessen før, under og etter at hendelsen fant sted, og i denne sammenhengen mener vi at du har relevant innsikt å komme med, som gjør at vi mener at det har stor verdi at du deltar

i dette forskningsprosjektet. Denne forespørselen er ikke noe vi har sendt til mange andre, på det meste ser vi for oss å be en håndfull personer delta på den måten vi ber deg om å delta.

Hva innebærer det for deg å delta?

Deltakelse innebærer at vi ønsker å utføre et eller flere intervjuer med deg, der lydopptak av intervjuet vil lagres. Intervjuet kommer til å bestå av et utvalg spørsmål knyttet til angrepet du har blitt utsatt for. Dette inkluderer hendelsesforløpet før, under og etter angrepet, tiltak du og andre aktører har gjort eller ikke gjort, både i forkant og etterkant av angrepet. Spørsmålene stilles kun for å forstå hvordan hendelsen kunne inntreffe, ikke for å fordele skyld eller liknende. Vi kommer ikke til å be deg om personopplysninger ut over ting som vedrører jobben din, og andre faktorer som er relevante for konteksten til angrepet.

Det er frivillig å delta

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

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrevet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

De som vil ha tilgang til opplysningene du oppgir vil være Maria Bartnes og Per Håkon Meland, veiledere fra NTNU, samt Silje Berg og Tilde Thorvik, som skriver den aktuelle masteroppgaven. Navnet ditt og annen personlig informasjon vil enten fjernes eller erstattes i presentasjonen av datagrunnlaget. Ved erstatning av personlig informasjon vil vi erstatte den personlige informasjonen med en kode som lagres på en egen liste adskilt fra øvrige data. Vi følger NTNUs retningslinjer for lagring av forskningsdata, og derfor vil datamaterialet lagres på NTNUs servere. Du som deltaker vil ikke kunne gjenkjennes i publikasjonen vår, med mindre dette er strengt nødvendig og vi inngår en enighet om dette på et senere tidspunkt. Dette har du naturligvis full bestemmelsesrett over selv.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er i midten av juni. Etter prosjektslutt vil personopplysninger og lydopptak fra intervju slettes

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

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

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

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

- NTNU ved Maria Bartnes (maria.bartnes@sintef.no), veileder for prosjektet, eller studentene Tilde Thorvik (tildegt@stud.ntnu.no) og Silje Berg (silber@stud.ntnu.no).

- Vårt personvernombud: Thomas Helgesen (epost: thomas.helgesen@ntnu.no, telefon: 930 79 038)

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

- Personverntjenester på epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Maria Bartnes
(Forsker/veileder)

Tilde Thorvik
(Student)

Silje Berg
(Student)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Social engineering attacks in the light of security economics*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i *intervju*
- at *opplysninger om meg publiseres slik at jeg kan gjenkjennes [beskriv nærmere] – hvis det blir aktuelt*

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

(Signert av prosjektdeltaker, dato)

Appendix **C**

Interview guide

This appendix shows the interview guide that was prepared for the interviews. One guide is for the security experts, while the other is for the social engineering victims. Not all questions were asked to every interviewee, either because they turned out to be less relevant, or the interviewee covered the topic unsolicited. The appendix is in Norwegian.

SPØRSMÅL TIL SIKKERHETSEKSPERTER:

Intro

Kan du starte med å fortelle litt om bakgrunnen din, og hva du jobber med?

SocEng trender, suksess

- 1) Hvordan ser trusselbildet for social engineering-angrep ut i dag?
- 2) Hvorfor tror du social engineering angrep til stadighet er suksessfulle?

Holdninger

- 3) Mørketallsundersøkelsen 2020 viser at 64% som blir utsatt av et sikkerhetsbrudd sier at grunnen var uflaks eller tilfeldighet, har du noen tanker rundt dette og hvorfor dette er en stor oppfatning blant folk?
- 4) Kan du beskrive sikkerhetskulturen i din organisasjon?
- 5) Mennesket blir ofte sett på som det svakestet leddet når det kommer til sikkerhet, hva er dine tanker om dette?
- 6) Har du noen eksempler på hvordan sikkerhetskulturen samsvarer med eller ikke samsvarer med kulturen i din organisasjon?

Tiltak

- 7) Hvilke tiltak er etter din mening de mest effektive for å redusere sannsynligheten for suksessfulle social engineering angrep?
- 8) Hvorfor tror du at tiltak mot social engineerings angrep ikke alltid fungerer som forventet i praksis?
- 9) Tror du at sikkerhets trening er nyttig? Hva tror du kan gjøres for å forbedre nyttigheten av det?
- 10) Insentiver handler i stor grad om hvilken motivasjon man har for å gjøre en handling. En mulig grunn til at det ikke legges tilstrekkelig innsats på riktig sted innenfor sikkerhet er misaligned incentives, som medfører at den som er i en posisjon til å forhindre et angrep, ikke har noen incentiver for å gjøre begrensede tiltak. Har du noen tanker rundt hvordan misaligned incentives mellom ulike aktører kan påvirke sikkerheten i et system eller mellom systemer?
- 11) Eksternaliteter er når en aktør utviser atferd som påvirker nytten til en annen aktør, uten å ta hensyn til kostnad/nytte for den andre parten. Eksempler er nettverkseksternaliteter, som at et sosialt medium får mer nytte for hvert enkelt medlem jo flere som blir med, og negative eksternaliteter, som en fabrikk som forurenser klima, men der konsekvensen av dette ikke legges inn i noe regnskap, og konsekvensen av forurensningen ignoreres. Har du noen eksempler på hvordan eksternaliteter påvirker sikkerheten i din organisasjon?

Økonomi

- 12) Noen risikoer må man akseptere, hva mener du man kan akseptere og hvor mye risiko mener du man kan akseptere?

SPØRSMÅL TIL OFRE

Om casen

- 13) Kan du fortelle om svindelen og hva skjedde?
- 14) Kan du beskrive prosessen, arbeidet og hva som har skjedd siden svindelen fant sted?
- 15) Vet du hvem som står bak angrepet?
- 16) Hvorfor tror du de gjorde dette?
- 17) Hvilke kostnader er forbundet med hendelsen? Både arbeidsressurser, penger, tid etc.

Forståelse og forebygging

- 18) Hvorfor tror du at du og de rundt deg ble ofre for et slikt angrep?
- 19) Hvorfor tror du angrepet lyktes?
- 20) Hvorfor tror du at tiltak mot social engineering angrep ikke alltid fungerer som forventet i praksis?
- 21) Før hendelsen fant sted, hadde dere noen prosedyrer som skal fungere som tiltak mot slike angrep? Har dere noen tiltak nå som skal forhindre en slik hendelse?
 - a) Hva kunne du gjort for å forhindre dette?
 - b) Hva kunne de andre aktørene gjort for å forhindre svindelen?
- 22) Tror du et slikt forsøk på angrep vil skje med dere igjen?
- 23) Har du fått noe bistand fra politi eller liknende aktører i forbindelse med svindelen? Er det noe du har satt spesielt pris på at har blitt gjort, eller noe du spesielt har savnet fra slike aktører?
- 24) Opplever du at det finnes tiltak du kan gjøre for å være sikker på at noe lignende ikke skjer igjen? Eller ligger slike tiltak hos en annen aktør? Har en eventuell annen aktør noen incentiver for å innføre tiltak for å forebygge denne typen angrep?
- 25) Vet du hvordan du kan gå frem for å skaffe deg informasjon om mulige tiltak mot slike angrep? / Synes du det er enkelt/vanskelig å finne informasjon om tiltak som kan beskytte mot slike angrep?
- 26) Incentiver handler i stor grad om hvilken motivasjon man har for å gjøre en handling. En mulig grunn til at det ikke legges tilstrekkelig innsats på riktig sted innenfor sikkerhet er misaligned incentives, som medfører at den som er i en posisjon til å forhindre et angrep, ikke har noen incentiver for å gjøre begrensende tiltak. Har du noen tanker rundt hvordan misaligned incentives mellom ulike aktører kan påvirke sikkerheten i et system eller mellom systemer?
- 27) Eksternaliteter er når en aktør utviser atferd som påvirker nytten til en annen aktør, uten å ta hensyn til kostnad/nytte for den andre parten. Eksempler er nettverkseksternaliteter, som at et sosialt medium får mer nytte for hvert enkelt medlem jo flere som blir med, og negative eksternaliteter, som en fabrikk som forurenser klima, men der konsekvensen av dette ikke legges inn i noe regnskap, og konsekvensen av forurensningen ignoreres. Har du noen eksempler på hvordan eksternaliteter påvirker sikkerheten i din organisasjon?

Holdninger

- 28) Før hendelsen fant sted, var angrep som dette noe du tenkte på i arbeidshverdagen?
- 29) Hvorfor er det viktig for dere at informasjon om denne hendelsen kommer/ikke kommer ut?
- 30) Hva synes du om tiltak som tofaktor-autentisering? Føler du at det har noen verdi, eller er det mest en frustrasjon å forholde seg til?
- 31) Mørketallsundersøkelsen 2020 viser at 64% som blir utsatt av et sikkerhetsbrudd sier at grunnen var uflaks eller tilfeldighet, har du noen tanker rundt dette og hvorfor dette er en stor oppfatning blant folk?
- 32) Mennesket blir ofte sett på som det svakestet leddet når det kommer til sikkerhet, hva er dine tanker om dette?

Oppfølgingsspørsmål

Oppfølgingsspørsmål til Security Expert A

- Så du mener det kan være vanskelig å vite hva ting er verdt?
- Konteksten er at vi har pratet med folk i bedrift X som er offentlig og har én type kultur, og pratet med folk i bedrift Q, som har en annen type kultur. Vi har merket at det er litt ulikt hva de fokuserer på, og du har jo innsikt i mange ulike bransjer og kulturer, om du kan si litt om hvordan du tror DET spiller inn på sikkerhetsvalg og økonomiske valg?
- Tror du det er noe bedriftene er bevisst på, det med hvordan den kulturen og holdningene er med og påvirker?
- I hvor stor grad tror du sikkerhets awareness program fungerer?
- Mener du tiltak som cyber insurance, policy adjustments eller bare å akseptere risiko kan ha verdi? Isåfall, hvilken verdi har de ulike løsningene?

Oppfølgingsspørsmål til Security Expert C

- Merker dere at folk er mer bevisst på det etter slike kampanjer?

Oppfølgingsspørsmål til Security Expert D

- Hva ønsker du å vite mer om selv?

Oppfølgingsspørsmål til Security Expert E

- Har du phishing-kampanjer eller lignende i din organisasjon? Hvorfor/ hvorfor ikke?
- Kan du beskrive hvordan finansteamet er strukturert, og hvordan dette bidrar til å redusere sannsynligheten for vellykkede sosial manipulasjons angrep?

Oppfølgingsspørsmål til Victim A

- Er dette noe dere har snakket med leverandøren om? Har de blitt spurt om de har blitt bedt om å oppgi slik informasjon til dere?

- Har dere sterkere rutiner for å takle dette nå?
- Føler du at åpenheten deres rundt denne saken har hatt noen negative eller positive virkninger på omdømmet til UiT?
- Likevel valgte dere å gå offentlig ut med det, hvorfor gjorde dere det, hva ønsket dere å oppnå med det?
- Dere har litt bevisst forhold til hvilke tiltak som er verdt det og ikke?

Oppfølgingsspørsmål til Victim B

- Dere også har et behov for å holde ting hemmelig for å ikke henge ut de andre partene?
- Det er policyen til de du jobber med at dette er ikke denne typen ting dere vil ha publisitet på.
- Du er jo en del av et miljø med folk som jobber med samme ting. Er dette noe dere har snakket om med andre i bransjen?
- Tror du det hadde vært nyttig å snakke mer om det internt i bransjen, gitt at man tar vekk frykten for at det kommer ut i media?

Oppfølgingsspørsmål til Victim C

- Du snakker om flere nye lover, hvilke sikter du til?
- Du nevner noe vi ser på, som handler om tillit. Tillit under pandemien har vært en ressurs siden folk stoler på hverandre og myndighetene, mens det du var ute for her, som rammer folk som stoler på folk og er snille, skulle du ønske at du var mindre tillitsfull? Eller ville det vært kjipere å ikke være så tillitsfull til tross for det du har opplevd?
- Du har gått ut offentlig og snakket om dette, hvorfor? Hva ønsker du å oppnå?
- Tror du skam er grunnen til at folk ikke er så åpne om dette, eller tror du det er noe annet som er grunnen til at folk synes det er flaut?
- Man møter ofte et kryss mellom brukervennlighet og sikkerhet, som også gjelder her mtp hvor lett det er å få lån etc. Kan du utdype om dine erfaringer med dette?
- Angrer du på at du har stått frem, eller føler du at det er verdt det?

Oppfølgingsspørsmål til Victim D

- Hvilke best practices bruker dere ikke?
- Tror du at sikkerhets trening er nyttig? Hva tror du kan gjøres for å forbedre nyttigheten av det?
- Er du mer aware nå?
- Vil du at selskapet ditt skal gjøre slike sikkerhets treninger?
- Ble du irritert over hendelsen? Eller ble andre i organisasjonen irritert?

Appendix **D** Coding

Examples of how we coded is illustrated in Figures D.1 and D.2. Figure D.1 gives an overview over codes used in the coding tool when interviewing Security Expert A. Figure D.1 shows how we collaborated with the coding and discussed how we could use the different findings. As illustrated, we used different colors to mark what we believed could be used as a statement and what we could use as paraphrasings.

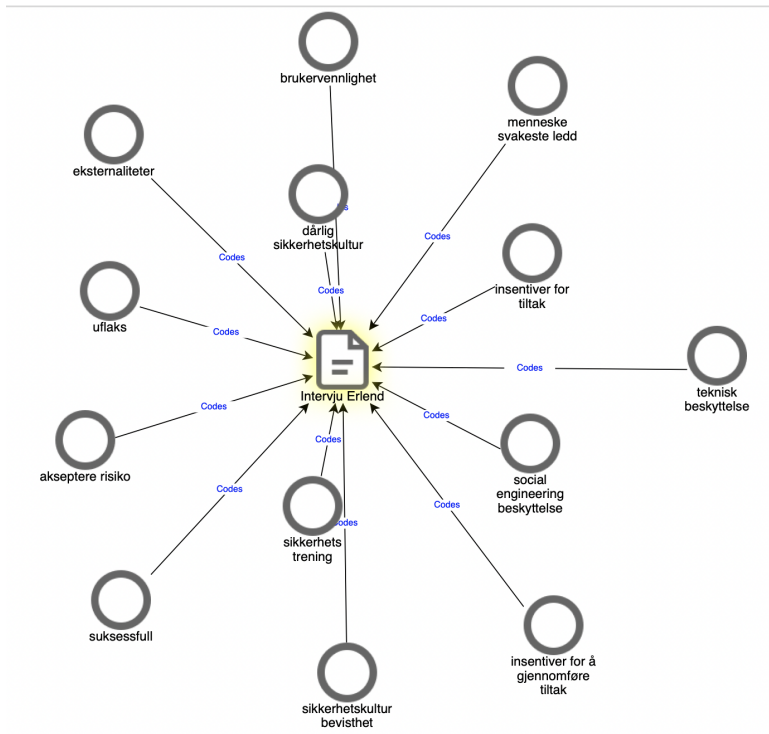


Figure D.1: Overview over codes in the coding tool used on the interview to Security Expert A

biblioteker som brukes, all softwaren man har, hvordan skal man ha sjanse til å holde styr på det. Så sikkerhet fatigue kan også ramme IT-folk fordi det er så store systemer. Men akkurat for social engineering er det tilliten det går ut på. Akkurat i Norge så er vi på andre plass på tillit i Europa. Det hjelper jo ikke på statistikken her i Norge.

T: tillit har vært en stor ressurs uten pandemien, men akkurat her så hjelper det ikke

- jeg er ikke for å drepe tilliten i Norge, men skanskje vi bør fokusere det på opplæring i stedet for å ha 8 eller 10 tegn i passordet ditt. Fokuser på at den du snakker med faktisk er den de utgir se for.

Tror du at sikkerhets trening er nyttig? Hva tror du kan gjøres for å forbedre nyttigheten av det?

- Full disclosure, vi selger ressurser for opplæring, så det kan ha en innvirkning på det jeg sier her. Jeg tror at sikkerhetsopplæring har vært preget av ingeniørenteking i den forstand at hvis vi skal nå ut med opplæring til mange, da må vi bruke e-læring. Og hva er e-læring, jo en nettside der du kan lese litt og se en video også er du ferdig. Skalrerer kjempebra, du kan rulle ut til 30 000 personer på en dag hvis du vil. Du kan skjule deg bak at det ikke er så mange som plager deg, du slipper unna med det. Det har en kostnad på produktiviteten. Men kanskje tilrettelegge opplæring der du har 2 timer lurer du på etat ta igjen bust

Siye Berg
ja!

SB Siye Berg
tillit som en grunn til at ting ikke funker i praksis og hvorfor angrep er suksessfulle
March 28, 2022, 11:30 AM

TT Tilde Gregusson Thorvik
veldig viktig! Tillit føler jeg hører til under RQ1 som eksternalitet, men denne er et godt eksempel på hvordan man kan se de RQ1 og RQ2 i sammenheng feks
March 28, 2022, 11:31 AM

TT Tilde Gregusson Thorvik
Sikkerhetskultur > spesifikke tekniske tiltak, føler det er noe vi kan ta opp under RQ4, at det enkleste for både
See more

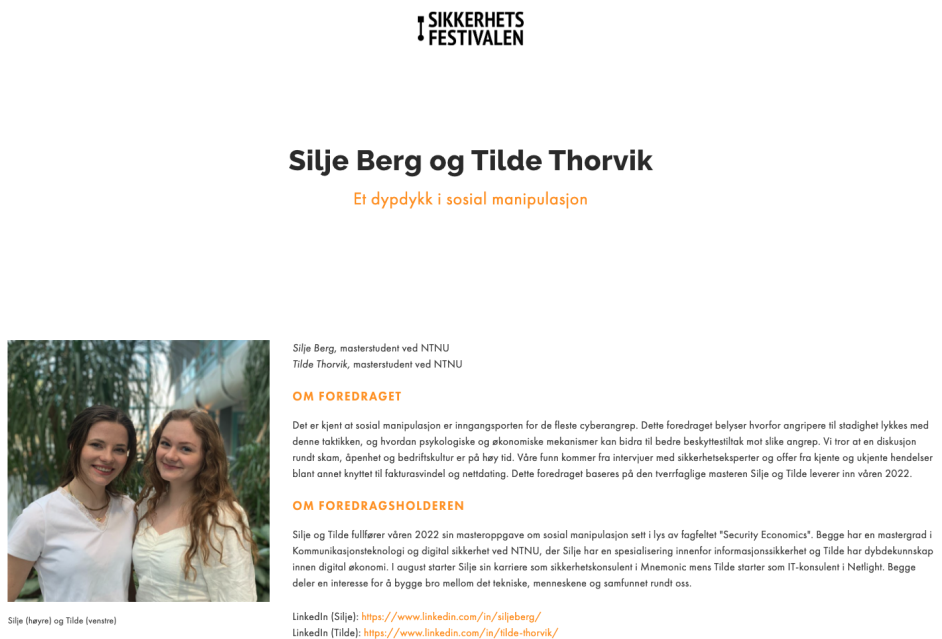
TT Tilde Gregusson Thorvik
INCENTIVER!!!!

Figure D.2: Example of how we worked together on coding the data

Appendix **E**

Admission to Sikkerhetsfestivalen 2022


Figure E.2 shows that we are accepted to *Sikkerhetsfestivalen 2022* to talk about this thesis. Figure E.1 shows the website that introduce our talk [68].



**SIKKERHETS
FESTIVALEN**

Silje Berg og Tilde Thorvik

Et dyddykk i sosial manipulasjon



Silje Berg, masterstudent ved NTNU
Tilde Thorvik, masterstudent ved NTNU

OM FOREDRAGET

Det er kjent at sosial manipulasjon er inngangsporten for de fleste cyberangrep. Dette foredraget belyser hvorfor angripere til stadighet lykkes med denne taktikken, og hvordan psykologiske og økonomiske mekanismer kan bidra til bedre beskyttelse mot slike angrep. Vi tror at en diskusjon rundt skam, åpenhet og bedriftskultur er på høy tid. Våre funn kommer fra intervjuer med sikkerhetsekspert og offer fra kjente og ukjente hendelser blant annet knyttet til fakturasvindel og nettdating. Dette foredraget baseres på den tverrfaglige masteren Silje og Tilde leverer inn våren 2022.

OM FOREDRAGSHOLDEREN

Silje og Tilde fullfører våren 2022 sin masteroppgave om sosial manipulasjon sett i lys av fagfeltet "Security Economics". Begge har en mastergrad i Kommunikasjonsteknologi og digital sikkerhet ved NTNU, der Silje har en spesialisering innenfor informasjonssikkerhet og Tilde har dybdekunnskap innen digital økonomi. I august starter Silje sin karriere som sikkerhetskonsulent i Mnemonic mens Tilde starter som IT-konsulent i Nellight. Begge deler en interesse for å bygge bro mellom det tekniske, menneskene og samfunnet rundt oss.

LinkedIn (Silje): <https://www.linkedin.com/in/siljeberg/>
LinkedIn (Tilde): <https://www.linkedin.com/in/tilde-thorvik/>

Silje (høyre) og Tilde (venstre)

Figure E.1: Introduction of our talk on *Sikkerhetsfestivalen 2022* [68]

Hei Siije,
Vi kan med glede informere deg om at ditt foreslåtte foredrag "Et dypdykk i sosial manipulasjon" til Sikkerhetsfestivalen 2022 er akseptert! Ditt foredrag er planlagt 30. august kl. 14:00. Det er satt av 30 minutter til foredraget. Vi ber deg planlegge innlegget ditt til 25 minutter, slik at det er 5 minutter til spørsmål. Vi planlegger å sende ut programmet rundt 1. April, **dermed ønsker vi at du sender oss denne informasjonen så snart som mulig.**

Figure E.2: Confirmation of acceptance to *Sikkerhetsfestivalen 2022*

