UiA University of Agder

Master

The Role of Social Media in Social Engineering Attacks

A Qualitative Study on Technical-, Individual-, and Organizational Measures to Mitigate Social Engineering Attacks in Social Media

CHRISTIAN SOLHEIM

DANIEL BERGMANN

SUPERVISOR

Professor Jaziar Radianti, University of Agder

University of Agder, 2024
Faculty of Social Sciences
Department of Information Systems

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	Ja
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	Ja
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	Ja
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	Ja
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	Ja
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	Ja
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	Nei

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	Ja
Er oppgaven båndlagt (konfidensiell)?	Nei
Er oppgaven unntatt offentlighet?	Nei

Acknowledgements

We want to express our sincere gratitude to our supervisor, Professor Jaziar Radianti from the Department of Information Systems at the University of Agder (UiA), for her valuable guidance and tremendous support throughout this master thesis. The continuous constructive criticism have been of massive help to us and instrumental for pointing us in the right direction of the thesis. Thank you once again for your unwavering support and encouragement - this would not have been possible without you.

We also want to thank the ten respondents that have been part of this master thesis, for their valuable time and efforts in their busy schedule. Their contributions of empirical evidence have been essential to the data collection and provided us with invaluable insight.

Lastly, we would like to thank our family and friends for their unwavering support throughout this master thesis. Their continued encouragement and motivation have been immensely important throughout the years of study, especially in this period of writing the master thesis.

Kristiansand,
June 6th, 2024

Christian Solheim

Christian Solheim

Daniel Bergmann

Daniel Bergmann

Abstract

It is estimated that 98 % of all cyberattacks include some form of social engineering (Rebeca, 2023). The continued relentless cyber-related threats to organizations are ever-growing and important to address to mitigate the risks of being attacked. Social media platforms could be considered as the perfect hunting ground for social engineers to scour user profiles for personal and exploitable information to either deceive users directly or use this information to plan for a future attack.

This research focuses on the role of social media in social engineering attacks, more specifically how social engineering can be mitigated from three perspectives: **1)** Technical measures that the social media platforms are responsible for implementing, **2)** User-related responsibilities, **3)** How organizations could facilitate the education and awareness training of their employees on the use of social media.

With this research being deductive-based, a systematic literature review (SLR) was conducted to build a foundation of literature of the relevant topics. For the empirical data collection, ten respondents from various international organizations were interviewed, including professionals and researchers in the field of cybersecurity and communication. The interviews were conducted with a semi-structured format. The Cybersecurity Culture Framework from (Gioulekas et al., 2022) was adopted throughout this master thesis, with it also being the foundation for the data analysis. As a result of the empirical findings and the Cybersecurity Culture Framework, it has emerged an inductive conceptual framework with new concepts.

Combining the results from both the literature review and the empirical findings, it is apparent that there are several measures, in all three perspectives, that are viable. From the platform and technical perspective, the use of some form of unique identification to remedy the risks of fake accounts and fraud, in addition to the use of AI to predict and prevent potential social engineering attacks is advised. Both from the individual- and organizational aspect, the common denominators are the high focus of training and awareness, both privately and professionally. This includes that users of social media have to familiarize themselves with the terms of use, and realize the consequences of sharing content and information on such platforms.

Contents

1 Introduction **1**
- 1.1 Research Approach . . . 2
- 1.2 Overview of The Thesis . . . 2

2 Background and Related Work **4**
- 2.1 Social Engineering . . . 4
  - 2.1.1 Tactics, Techniques and Procedures (TTP) . . . 5
- 2.2 Social Media . . . 6
  - 2.2.1 Social Media and Social Engineering . . . 7
- 2.3 Technical Countermeasures . . . 7
  - 2.3.1 Artificial Intelligence (AI) . . . 7
  - 2.3.2 Policies . . . 9
  - 2.3.3 Unique Identification . . . 10
- 2.4 Non-Technical Countermeasures . . . 11
  - 2.4.1 Awareness . . . 11
- 2.5 Summary and Literature Gap . . . 12
- 2.6 Conceptual Framework . . . 13
  - 2.6.1 Cybersecurity Culture Framework . . . 13
  - 2.6.2 Our Model . . . 14
- 2.7 Related Work . . . 15
- 2.8 Limitations and Assumptions Based On The Literature . . . 17
  - 2.8.1 Social Engineering . . . 17
  - 2.8.2 Social Media . . . 17

3 Methodology **18**
- 3.1 Systematic Literature Review (SLR) . . . 18
  - 3.1.1 Method . . . 18
  - 3.1.2 Review Protocol . . . 19
  - 3.1.3 Literature Search . . . 20
  - 3.1.4 Screen For Inclusion . . . 21
  - 3.1.5 Quality Assessment . . . 21
  - 3.1.6 Literature Search Result . . . 21
- 3.2 Research Approach . . . 22
  - 3.2.1 Qualitative Approach . . . 22
  - 3.2.2 Rationale For The Qualitative Approach . . . 23
- 3.3 Intellectual Reasoning . . . 24
- 3.4 Research Design . . . 25
- 3.5 Data Collection . . . 26
  - 3.5.1 Semi-Structured Interviews . . . 26
  - 3.5.2 Respondents . . . 26
  - 3.5.3 The Interview Process . . . 27
- 3.6 Data Analysis . . . 28

3.6.1 Transcription . . . 28
3.6.2 Coding . . . 28
3.7 Limitations, Ethical Considerations and Potential Challenges . . . 29
3.7.1 Challenges in Data Collection . . . 29
3.7.2 Challenges in Data Analysis . . . 30
3.7.3 Ethical Considerations . . . 31

4 Empirical Findings **32**
4.1 Trust and Risk Associated With Social Media . . . 32
4.1.1 Trust . . . 32
4.1.2 Risk . . . 33
4.2 Platform . . . 34
4.2.1 Technical Possibilities . . . 34
4.2.2 Artificial Intelligence (AI) . . . 35
4.2.3 Implemented Platform Security and Economics Interests . . . 36
4.2.4 Interrelation between Technical and Human Aspects . . . 37
4.3 Individual . . . 37
4.3.1 Responsibility . . . 37
4.3.2 What Should Users Actually Do? . . . 38
4.3.3 Enabling Security Controls . . . 39
4.3.4 Education and Awareness from an Early Age . . . 39
4.3.5 Differences in Physical and Abstract Experiences . . . 40
4.4 Organization . . . 40
4.4.1 Organizations and Their Employees Role . . . 40
4.4.2 Training and Awareness . . . 41
4.4.3 Rules and Policies . . . 43
4.4.4 Top Management . . . 44

5 Discussion **46**
5.1 Inductive Conceptual Framework (ICF) . . . 46
5.2 Platform . . . 47
5.2.1 Access and Trust . . . 47
5.2.2 Defense . . . 49
5.2.3 Security Governance . . . 50
5.3 Individual . . . 50
5.3.1 Awareness . . . 50
5.3.2 Competency . . . 52
5.3.3 Behavior . . . 52
5.4 Organization . . . 53
5.4.1 Defense . . . 53
5.4.2 Behavior . . . 55
5.4.3 Operations . . . 55
5.5 Implications . . . 56
5.6 Limitations of This Thesis . . . 57
5.7 Future Research . . . 57

6 Conclusion **58**

Bibliography **61**

Appendices **65**
A Interview Guide 65
B Consent Form 67
C Overview of SLR articles 71

List of Figures

2.1 Figurative representation of the Cybersecurity Culture Framework (Gioulekas et al., 2022) . . . 13
2.2 Our conceptual framework based on Gioulekas et al. (2022)'s Cybersecurity Culture Framework . . . 14
2.3 Phase-based model of Social Engineering attacks in SNSs (Algarni & Xu, 2013, p. 458) . . . 15
2.4 Source-based model of Social Engineering attacks in SNSs (Algarni & Xu, 2013, p. 650) . . . 16

3.1 The systematic literature review process (Xiao & Watson, 2019, p. 103) . . . 19
3.2 Overview of keywords used in SLR . . . 20
3.3 Overview of the literature search result . . . 22
3.4 Research design decisions (Recker, 2021, p. 45) . . . 25

5.1 Inductive conceptual framework with categories and adherent concepts . . . 46

List of Tables

3.1 Overview of the key aspects in "Some contrasts between quantitative and qualitative research" (Adapted from (Bryman, 2016, p. 401)) 23
3.2 Overview of respondents and their job title 27

Chapter 1

Introduction

An ever-growing threat to organizations, regardless of their size and scale, is the relentless attempts of cyberattacks and fraud, including social engineering that could act as both a direct attack method, but also a way to gain information to plan for a future cyberattack (Rebeca, 2023). It is estimated that 98 % of all cyberattacks include some form of social engineering at one or several stages in the cyber kill chain (Rebeca, 2023). The origins of social engineering can be traced back to the mid-1800s, being the intention to alter or manipulate the mindset of an individual or a group of people for the attacker's own advantage (Hatfield, 2018, p. 103–110).

Social media platforms have become one of the most efficient and practical ways of communicating with people all over the world, both privately and professionally (Rudra, 2023). The type of information and content that is being shared varies from beneficial content to harmless jokes and other personal- and contact information. With the large number of users on social media platforms, they could be considered the perfect hunting ground for attackers to either conduct social engineering attacks or use the platforms as a way to gather information.

A common way for social engineers to manipulate and deceive their targets on social media is through impersonation, usually by the means of fake- or compromised accounts (Rudra, 2023). The aim of the social engineers vary, but is usually financially driven, where the personal- and sensitive information can be sold or used for a different purpose (Rudra, 2023). With the large quantities of personal- and sensitive information available through social media platforms, and the relentless attempts of social engineering attacks, it is important to emphasize measures of mitigation and how to decrease the number of successful attacks to prevent financial loss, for both individuals and organizations.

Neither social engineering nor social media are new areas of study. Algarni and Xu (2013) have been investigating how social engineers perform attacks against users on *Social Networking Sites*, which was the term for social media at that point in time. However, there is a lack of research done on the combination of these two topics, which we have identified as a research gap that we aim to contribute towards. While Algarni and Xu (2013) look at the topic from an social engineer's point of view, we aim to investigate the role of social media in social engineering attacks, more specifically how social engineering can be mitigated from three perspectives: technical, individuals, and organizations.

We believe that researching the topic with a more holistic approach would be highly insightful as it encompasses important aspects from the three perspectives. First of all, the technical possibilities of the social media platforms, secondly what the average Jane and Joe have to be aware of and consider when using social media platforms, and lastly looking at how organizations could facilitate the education and awareness training of their employees on the use of social media. The research questions are as follows:

> **RQ1:** *Which technologies and measures exist to help secure users of social media platforms from social engineering attacks?*
>
> **RQ2:** *What responsibilities lie on the users of social media platforms to protect themselves against social engineering attacks?*
>
> **RQ3:** *How can organizations educate their employees in safe use of social media to reduce the occurrence of social engineering attacks?*

1.1 Research Approach

To answer our three research questions, we have conducted a qualitative research study. This master thesis consists of various methods, starting off with a systematic literature review, where we collected, synthesized and analyzed literature and articles which was relevant for this research project. The results from this literature review, which is presented in the upcoming section 2, defines and presents the core concepts of this thesis, which are combined with the empirical findings to conclude on the research questions.

To structure the research project, we have adapted the Cybersecurity Culture Framework from (Gioulekas et al., 2022). We have derived from the original framework, where we have adopted certain concepts and created our own version. This framework have been present throughout the project, starting from the planning phase and creation of interview questions, to reporting and discussing the findings. The adopted version of the framework is presented in figure 2.2. Furthermore, in chapter 5, we present an inductive conceptual framework, to include the new emerging concepts identified through the empirical data analysis.

To collect the empirical data needed to answer the research questions, we have opted for a qualitative research approach, using semi-structured interviews. In total, we have been interviewing ten different professionals between February and April of 2024, including people working with cybersecurity or social media, as well as researchers and experts from both fields.

1.2 Overview of The Thesis

Chapter 1 - Introduction provides an overview of the research areas and problems related to this thesis, as well as the rationale for scrutinizing this topic.

Chapter 2 - Background and related work presents the results from the systematic literature review, as well as the inclusion of the conceptual framework, which is adopted throughout this study.

Chapter 3 - Methodology explains the research approach which have been the focus throughout the work on this thesis, along with the motivations and rationale for this approach.

Chapter 4 - Findings presents the empirical results, gathered from the semi-structured interviews. These findings are structured according to the conceptual framework.

Chapter 5 - Discussion is similarly structured according to our conceptual framework, and includes the discussion of the findings from the interviews together with the findings from the literature review. The implications and limitations of the thesis are addressed, as well as suggestions on how this topic can be further researched.

Chapter 6 - Conclusion aims to provide the main takeaways from the three research questions of this thesis.

Chapter 2

Background and Related Work

In this chapter, we present the findings from our systematic literature review process (SLR). This includes defining and explaining core concepts that are central or closely related to the research topic. In the first section, we will cover the concept of social engineering, including different tactics, techniques, and procedures (TTP). Furthermore, we will look into what social media is, and how threat actors could make use of it to their advantage. Section two of the literature findings will cover different countermeasures against social engineering, from a technical, individual and organizational perspective. The process and practical application of the systematic literature review will be explained in section 3.1. The overview of the articles used in this section is included in appendix C.

2.1 Social Engineering

Social engineering is quickly becoming one of the most lucrative and effective ways for threat actors to attack their victims (Hylender et al., 2023, p. 8). Statistics from 2023 narrate that the human element is a dominant factor in cyberattacks, with 74% of all investigated cyber incidents reveal the human element as a point of entry for an attacker (Hylender et al., 2023, p. 8). The statistic of the reported 98 % of all cyberattacks including some aspect of social engineering, is not representative of social engineering and human aspect being the responsible factor for point of entry for an attacker (Rebeca, 2023). In the realm of cybersecurity, social engineering can be seen as a type of attack where attackers exploit human vulnerabilities to gain access to sensitive information through social interactions with their victims (Wang et al., 2020, p. 85105). The information collected from social engineering attacks can often be highly sensitive, and it can be enough to breach someone's cybersecurity, both individuals or organizations (Wang et al., 2020, p. 85105).

Even though social engineering is mostly known in regard to cybersecurity, it is not a new phenomena. The concept of social engineering has from its roots all the way back in 1842, up until the 1940's been based on three core principles, *Epistemic asymmetry*, *Technocratic dominance* and *Teleological replacement* (Hatfield, 2018, p. 103–104). These core principles are still present in today's day and age, being the foundation for the basics of social engineering.

Epistemic asymmetry refers to the gap in knowledge between people, when one person has a higher level of knowledge than others in a specific domain (Hatfield, 2018, p. 103). The second core principle, *technocratic dominance*, is strongly associated to *epistemic asymmetry*, and refers to a technocrat, a person who possesses technical expertise in a certain field, either in form of knowledge or skill. *Technocratic dominance* occurs when a technocrat uses their expertise to change the behavior of other people or groups. The third and final core principle is *teleological replacement*, where an attacker manages to replace a person's or

group's purpose or goal, with their own, utilizing *epistemic asymmetry* and their *technocratic dominance* (Hatfield, 2018, p. 103–104).

Today, we are witnessing a wide variety of techniques associated with social engineering. The majority of them are closely related and quite similar, where they also include the three core principles explained above (Hatfield, 2018, p. 108). Threat actors will use their *epistemic asymmetry* combined with *technocratic dominance* to trick victims with a lower degree of knowledge on a specific area into providing the threat actor a variety of valuable information, which can be further used to carry out an attack. In phishing scams, we often see that threat actors contact potential victims with lower technical knowledge than themselves, trying to utilize the asymmetry in knowledge between them, by asserting their *technocratic dominance* upon the victim. In the case of a successful phishing attack, threat actors are able to change the victim's behaviour, either by making them give away their username and password, sensitive information or other information that may be of the threat actor's interest, essentially being *teleological replacement* (Hatfield, 2018, p. 107–110).

In social engineering, threat actors apply methods like *deception*, *manipulation*, *persuasion*, *influence* and *induction* to trick their victims (Wang et al., 2020, p. 85106). This differ from other more traditional types of cyberattacks, where threat actors try to exploit system vulnerabilities, like brute-force attacks for gaining access to a user account or exploiting software vulnerabilities (Wang et al., 2020, p. 85106).

2.1.1 Tactics, Techniques and Procedures (TTP)

Threat actors use a variety of different techniques for social engineering attacks; Wang et al. (2020) describe twelve different attack methods, which includes some of the more traditional and well-known techniques, such as *Phishing* and *Pretexting*, along with some lesser known techniques, such as *Baiting* and *Water-holing* (p. 85110). The different techniques can be further divided into two categories, social- and socio-technical approaches (Breda et al., 2017, p. 3–5). According to Breda et al. (2017), the social approach includes techniques that rely mostly on the social interaction between people, like *tailgating* and *pretexting*, while the socio-technical approach includes techniques that combine both social and technical aspects, like *phishing* and *water-hole* (p. 3–5). We have decided to focus on techniques related to the research area of social media.

Pretexting

Pretexting is one of the most dominant social engineering techniques (Hylender et al., 2023, p. 31). Pretexting is an attack vector utilized in more than 50 % of the registered social engineering attacks in 2023 (Hylender et al., 2023, p. 8). In pretexting attacks, the threat actor presents the victim with a pre-made scenario or text, in combination with the attacker impersonating either a well-known and trustworthy person or an organization (Breda et al., 2017, p. 4). The use of text instead of other more technical tools or techniques, makes this type of technique to fall into the social approach (Breda et al., 2017, p. 4).

Phishing

Along with the aforementioned pretexting technique, phishing keeps on dominating the social engineering attack genre, with it being used in 44 % of all social engineering attacks in 2023 (Hylender et al., 2023, p. 31–32). During phishing attacks, threat actors combine both social- and technical techniques to steal their victim's personal or sensitive information (Gomes et al., 2020, p. 2). Threat actors use several types of methods to deliver their attacks, with email being the most well-known and common method (Gomes et al., 2020, p. 2).

In phishing attacks, the threat actors pretend to be someone trustworthy, like a trusted person or a well-known organization asking for confidential information from the victim, like username, password, bank details, or making them click on a link to access a fake site, where the victim can enter the demanded information (Gomes et al., 2020, p. 2). Threat actors tailor phishing attacks to target a larger population of potential victims, aiming to reach as many individuals as possible (Breda et al., 2017, p. 5). Phishing, as a technique, can be defined as a socio-technical technique, based on its use of both social- and technical techniques to manipulate the victims (Breda et al., 2017, p. 5).

Spear-phishing

Spear-phishing is a branch off phishing, where spear-phishing attacks are more targeted towards specific individuals or organizations (Breda et al., 2017, p. 5). Spear-phishing attacks require extensive research on the targets, to best tailor the content towards the specific victim (Breda et al., 2017, p. 5). Threat actors often use *Open Source Intelligence (OSINT)* to gather the required information on the targets, usually through social media, company websites or other information sharing platforms (Wang et al., 2020, p. 85110). OSINT refers to gathering and processing information that are found through publicly available sources (Lindemulder & Forrest, 2024). Similar to phishing, spear-phishing makes use of a combination of social- and technical methods, hence being labeled as a socio-technical method.

2.2 Social Media

The definition of the term *Social Media* is an ever-changing subject, with its reported roots back to Tokyo, Japan in 1994 (Aichner et al., 2021, p. 215). Despite the roots in Tokyo, Japan, the first social media platform is considered to be *SixDegree.com*, three years later (Boyd & Ellison, 2007; Wang et al., 2020). Furthermore, the first social media platform to gain a global audience is *mySpace* (Boyd & Ellison, 2007, p. 216–217). At that time, in the later stages of the 1990's, the term *Social Networking Sites* was used, instead of what we know it as today, *Social Media* (Wang et al., 2020, p. 85101).

Aichner et al. (2021) have conducted a thorough review to which they have identified the change in definition of the term *Social Media* from 1994 to 2019 (p. 215–222). In the earlier years of social media, it was often referred to as *Virtual communities*, *Computer-supported social networks* or *Social Networking Sites* (Aichner et al., 2021; Boyd & Ellison, 2007; Wang et al., 2020). It was not until 2010 the term *Social Media* was used explicitly (Aichner et al., 2021, p. 218–219).

There is no common consensus in terms of what social media actually is, and the definition will often be tailored to what the writer or researcher aims to contextualize social media with. Despite this, Wolf et al. (2018) try to describe the common denominators that contributes to the construct of social media (p. 3). Some of these pillars are that social media is built on a web-based application where the users are allowed to create profiles and interact with other users of the platform for sharing content, having conversations, forming groups and so on (Wolf et al., 2018, p. 3). Furthermore, *Web 2.0* is often referred to in relation to social media. Similar to social media, Web 2.0 encompasses a variety of concepts, but can be reduced to as the second generation of the Web, where the emphasis on the user is predominant, where the responsibility on providing content, information, collaboration, etc. lies on the users (Wilson et al., 2011, p. 1–2). One last standout, when it comes to the common denominators of social media, is the integration of information technologies that enables interaction and networking between users (Wolf et al., 2018, p. 3).

2.2.1 Social Media and Social Engineering

Where social media came to be very popular, attracting people from all over the world to create their own account and follow the trend, the amounts of data have grown rapidly (Wang et al., 2020, p. 85101). Social media platforms, such as Facebook, have over 30 billion posts or some kind of data sharing each month, generated by their users (Abu-Nimeh et al., 2011, p. 23). There are a plethora of data or information that users of the social media platforms share, such as relationship status, your recent activities, your whereabouts etc. (Wang et al., 2020, p. 85101). Other information that could be found through scratching the surface area of an account could reveal information like phone number, email address, work- and home addresses etc. In essence, social media have become a platform where malicious actors are able to scour accounts for information and manipulating the users to disclose other sensitive information that could be exploited (Wang et al., 2020, p. 85101–85102). Some of the most effective ways for a malicious actor to gain information from a user of social media, is to make the users gain a feel of (1) victory or excitement, (2) fear of authority or (3) fear of loosing something of value (Aun et al., 2023, p. 4918).

People of all ages are getting into social media, also seniors over the age of 65 are represented in the group of users of social media (Narayanan et al., 2021, p. 297). These seniors, that have not had social media as a part of their earlier years of life, are particularly more vulnerable when it comes to cyberattacks and does not necessarily possess the required knowledge of the potential risks and damages it could lead to. Although seniors are considered to be the most vulnerable group (Narayanan et al., 2021, p. 297), it do not mean that cyberattacks does not occur in younger age groups. The domain of disinformation, which essentially is the creation of false information to spread this with the intention to deceive or collect information from the ones who engages with it, is an area that most people will encounter, regardless of their age (Caramancion, 2020, p. 440–442).

2.3 Technical Countermeasures

Where we now have covered our main concepts with Social Engineering and Social Media, we will present some technical countermeasures that could be implemented to help social media platforms secure their users better.

2.3.1 Artificial Intelligence (AI)

When it comes to the subject of AI, and how to apply AI as a countermeasure to cyberattacks in social media, the sub-term *Machine learning* is often referred to (Thuraisingham, 2020, p. 1116–1118). A possible area of utilization for machine learning could be to detect malware and fake news (Homsi et al., 2021; Thuraisingham, 2020). These two are closely related, as fake news could potentially be derived from malware. The risk of malware is significant, where you never know the extent of it. Malware software could potentially create fake profiles, where fake posts and false information could be shared. This makes the detection of fake news imperative to mitigating a large amount of potential cyberattacks (Thuraisingham, 2020, p. 1116–1117).

In the world of business, fake accounts could potentially lead to loss of money, reputation, and legal issues that have to be dealt with (Homsi et al., 2021, p. 88). To decrease the number of fake accounts and mitigating the risk for an organization to be harmed, due to fake accounts, could machine learning also be used to detect fake accounts. Researchers, e.g., Homsi et al. (2021) and Kavin et al. (2022), have been exploring the possibilities for detecting fake accounts through machine learning.

On the topic of fake accounts - automated bots are also a method that could create a fake account and mimic or simulate human behavior on social media, which could be very challenging to detect for the systems, while also being difficult to distinguish between real- and fake accounts for users of social media (Homsi et al., 2021; Kavin et al., 2022). Gamallo and Almatarneh (2019) and Hai Wang (2010) discuss certain methods for detecting bots in social media platforms. Gamallo and Almatarneh (2019) describe the use of *Naive-Bayesian Classification*, which is a supervised machine learning algorithm, with an accuracy between 70 % and 88 %, depending on which language and other configurations, based on a Twitter training dataset provided by PAN Shared Task, while they also mention several cases with an accuracy of 95 %, but with the use of datasets that the researchers themselves had built (p. 1–3). PAN, in PAN Shared Task, is an organization that organizes annual scientific events and provides shared tasks on digital forensics for researchers to test their developed algorithms (PAN, n.d.).

Following, we will present some of the more directly social media-related countermeasures in the realm of AI.

Natural Language Processing

Natural language processing (NLP) branches off the domain of AI, which includes several methods that enables computers to process text and words, e.g., in order to interpret the context or predict potential outcomes, through machine learning (Carley, 2020; IBM, n.d.). In relation to social media and social engineering, NLP could be used as a tool to help and detect fake news (Mughaid et al., 2022), analyzing posts concerning specific topics or groups (Sliva et al., 2019), and also the attempt to understand the social media network's understanding and level of knowledge on specific subjects (Rodriguez & Okamura, 2019). Even though this might not be a countermeasure to social engineering attack directly, by the means of preventing a social engineer to attack a user of social media, it could be used to try and understand the bigger picture and potential harmful events in the real world.

The application of NLP may vary based on what the respective projects call for, whether it being detection of spam or fake news, translation applications, e.g. Google Translate, or sentiment analysis to gain insight into certain topics or groups in social media (IBM, n.d.). As a standard, the *Natural Language Toolkit* (NLTK)-library includes several methods for applying NLP for your needs. This open-source library contains programs built on Python, where developers are able to adjust the code to suit their requirements and needs for their application (IBM, n.d.).

With NLP being the umbrella term for a variety of methods, we have identified that *Sentiment analysis* has become a popular method to gain more insight into social media channels.

Sentiment Analysis

Sentiment analysis in social media, also called *Opinion mining*, is the process of analyzing the expressed posts, opinions and actions tied to certain topics, events and other public entities (Yue et al., 2019, p. 617–618). There are three main aspects for sentiment analysis, with the first one being for commercial advantage (Yue et al., 2019, p. 618). Organizations could use sentiment analysis as a part of mapping the product opportunities, essentially which areas have too extensive coverage, bad coverage or not interesting to people, and the area in between that both satisfies customers and is of importance (Jeong et al., 2019, p. 282). It could also aid e-commerce platforms' in-depth data into their products and services, which could be a part of enhancement of their products or system (Yue et al., 2019, p. 618).

The second aspect is the political context, where sentiment analysis could be used to get an overview of the people's political opinions and expressions (Yue et al., 2019, p. 618). An example could be a president election in the US, a sentiment analysis could be performed, which could give an indication of the state's ideological preference or tendency. Another example could be to map the perceived opinions on certain political individuals, either restricted to an array of languages or countries to narrow down the number of posts to some degree (Yue et al., 2019, p. 618–619).

The third aspect is public security, with the potential detection of upcoming real-life terrorist attacks and cyber attacks (Sliva et al., 2019; Yue et al., 2019). By analyzing certain social media channels, one may be able to predict and prevent possible cyberattacks, in addition to retrieve information on the recruitment of respondents for larger-scale hacktivist groups and attacks (Sliva et al., 2019, p. 638).

2.3.2 Policies

Moving on from the aspect of AI, one of the most common and dangerous threats, in the realm of technology and Internet, is the cyber-criminals' use of Internet to manipulate users into providing their login-credentials, in numerous ways (Osuagwu et al., 2015, p. 91). In terms of an organization mitigating the potential of a cyber-attack occurring, the definition of policies, to which describe the expected or desired behavior of the employees, should be in place (Osuagwu et al., 2015, p. 92). We will now provide some of the well-known and applied policies and countermeasures that users of all kinds of systems or other platforms encounter: *Passwords* and *Multi-factor authentication*.

Passwords

The use of passwords is considered the most frequent and popular way of user authentication, as the implementation is inexpensive and effective (University of Houston - Clear Lake, n.d.). A report from Nasjonal Sikkerhetsmyndighet (NSM), the Norwegian National Security Authority, called "Ti sårbarheter i norske IKT-systemer", they include some aspect of password in four of the ten vulnerabilities presented (NSM, 2023b, p. 7–10). This consists of weak passwords, brute force or password guessing, standard passwords and unprotected passwords in plain text. The emphasis on having strong password policies as a countermeasure, is also described in NSM's "Risiko 2023"-report (NSM, 2023a, p. 23). Osuagwu et al. (2015) further point out the importance of changing passwords, in addition to not using the same password for multiple accounts (p. 99).

For social media platforms, it may be difficult, dare say impossible, to make sure that their users have their own unique password for that specific account. Social media should have a password policy, which enables them to, e.g., encourage their users to have strong passwords by having certain requirements when both creating and updating the account's password, but still to a degree that people do not find it too extensive (NSM, 2023b, p. 7).

Multi-Factor Authentication

In addition to having a solid password policy, the implementation of multi-factor authentication (MFA) is also recommended (NSM, 2023a, 2023b). Systems that do not make use of MFA, are often more susceptible for brute force or password guessing attacks. Through NSM's testing of Norwegian ICT-systems, they rarely encounter MFA, furthermore the massive number of queries that a brute force attack produces, is rarely detected and dealt with by these systems (NSM, 2023b, p. 8).

There are numerous methods for MFA, but it has a minimum of two requirements or steps for a successful authentication (Kosinski & Forrest, 2024). This is usually by the means of password as the first requirement, along with either an authentication application, single-use passcode, biometrics or other physical devices as the second requirement. A combination of these factors could also be a possibility, depending on the sensitivity levels of the systems, in addition to the types of authentication factors in use (Kosinski & Forrest, 2024).

2.3.3 Unique Identification

Moving on from policies, more towards a potential universal project, we have *Unique Identification* (UID). UID refers to the process of providing every resident of a country with a unique identifier, e.g., social security number (Osuagwu et al., 2015; Rengamani et al., 2010). In the US, the federal government have considered to move away from the social security number, towards a unique identification method with the use of biometrics, e.g., facial recognition, fingerprint, and iris scanning (Rengamani et al., 2010, p. 147–149).

Osuagwu et al. (2015) recommend the use of unique national identification, as part of several other measures to help mitigate social engineering; more specifically in relation to mobile phone SIM registration, where all residents, including cybercriminals, have to register with their unique identification, in order to complete the registration (p. 99). This is merely a recommendation from Osuagwu et al. (2015)'s perspective rather than a description of the reality, but is still part of their recommendations based on their extensive analysis.

From a domestic point of view, in Norway, with the implementation of BankID, in combination with the social security number, for purposes such as online authentication, where ensuring your identity is crucial, has this been widely considered as successful. BankID is a Norwegian solution for authentication for the Norwegian citizens, where they authenticate themselves through the use of social security number, an authentication application, and a personal password for digital services (BankID, n.d.).

Whether this could be a universal solution for several countries, at least some kind of unique identification system, would depend on the financial state of the country, in addition to the population, along several other factors, both technological challenges and when it comes to the infrastructure of the country (Rengamani et al., 2010, p. 148–152).

Rengamani et al. (2010) describe that introducing biometrics into UID, in the name of the technical aspect, is that where only one single biometric measure is implemented, it may not meet its requirements and therefore lead to the user being unable to authenticate him- or herself (p. 149). As a result of this, multiple biometric measures could be used in combination with one another. Where this could again be a challenge, would be in light of a social concern with the potential misuse of biometric information; an overall privacy concern.

2.4 Non-Technical Countermeasures

Now that we have highlighted the use of technical- and organizational countermeasures, we will take a closer look into the realm of non-technical countermeasures. In this section, we will look at the importance of the users themselves, in addition to the importance of raising their awareness level, and present the recommended ways of sharing this information.

2.4.1 Awareness

We have earlier scratched the surface of Verizon's data breach report for 2023, where they conclude that the human element plays a significant part in successful cyber attacks, with 74% of all investigated cyber incidents including some form of human element, including social engineering (Hylender et al., 2023, p. 8). Threat actors have shifted their focus more towards humans as their main targets for cyberattacks (He, W. and Zhang, Z. J., 2019, p. 249). Having state of the art security technologies might not be enough to protect your company, if their employees are not trained and educated well enough on the constant threats of cybersecurity (He, W. and Zhang, Z. J., 2019, p. 249).

Training

The importance of educating and training employees are increasing (He, W. and Zhang, Z. J., 2019, p. 249). A number of organizations have already started the work of educating and training their employees, aiming to make their employees more aware and responsible, in regards to cybersecurity. Even though more organizations utilize training and awareness programs, and campaigns, both small and large organizations still suffer from cyberattacks (He, W. and Zhang, Z. J., 2019, p. 249).

He, W. and Zhang, Z. J. (2019) present nine core ideas to help organizations to create successful training programs (p. 252). These nine ideas are *Accountability*, *Fun*, *Hands-on*, *Interactivity*, *Just-in-time training*, *Personalization*, *Reinforcement*, *Relevancy* and *Reward* (He, W. and Zhang, Z. J., 2019, p. 252–253). He, W. and Zhang, Z. J. (2019) argue that these nine ideas will help organizations make a more engaging, fun and relevant cybersecurity training program, which can further encourage employees to attend and to improve their knowledge of cybersecurity, as well as their awareness and behavior (p. 255).

According to He, W. and Zhang, Z. J. (2019), there are a five key reasons for the awareness programs to not be as influential or successful as planned, with employees feeling bored during the awareness programs, being the first reason (p. 250). Training programs that are heavily focused on information regarding policies and procedures, are often being considered boring by the employees. Secondly, a lot of employees lack the motivation and enthusiasm needed to participate and complete the organizations' training and awareness programs, often because of a lack of incentives or rewards for participating. Furthermore, many employees feel that the training programs are not relevant for the company or their own job role; they could often get a feeling that the training programs are to generic (He, W. and Zhang, Z. J., 2019, p. 250).

Training programs also need to take all employees into account - different employees need different learning styles, and all content might not be applicable for all employees in an organization (He, W. and Zhang, Z. J., 2019, p. 250). Lastly, all training programs need to be revised and updated on a regular basis. The field of cybersecurity is always evolving and changing, making it a necessity to update the training program regularly, based on both the ever-changing cybersecurity landscape, as well as taking the respondents feedback into consideration (He, W. and Zhang, Z. J., 2019, p. 250).

Digital-PASS

A more specific countermeasure tailored towards users of social media platforms, is the learning platform called Digital-PASS. McHatton and Ghazinour (2023) describe a learning platform where users can explore and learn about the cyber threats that are present on social media platforms today (p. 30). Digital-PASS is a gamified simulation-based platform, where the users can play through different social media scenarios, either as a social media user or a hacker. The users of Digital-PASS will gain valuable insight into how hackers look for information, and how they use the information they are able to retrieve. When playing as a social media user, they get valuable insight regarding what information they potentially can and should not share, along with tips and advice to help them learn. Digital-PASS has been through several phases of testing since 2018, and have received positive feedback for being very realistic, as well as the testers showing increased awareness levels after testing and using the platform (McHatton & Ghazinour, 2023, p. 30).

2.5 Summary and Literature Gap

For the technical countermeasures, these are mostly focused on what the social media platforms could potentially implement as part of their security measures towards countering social engineering on their platforms. The likes of policies, including passwords and multi-factor authentication, could also be considered part of an organization's effort towards reducing the occurrence of social engineering attacks towards their employees on social media. Considering the non-technical countermeasures, with the inclusion of training and awareness, this is tailored towards organizations, whereas the gamified learning platform, Digital-PASS, could be both for organizations and individual users.

When it comes to the individual responsibility aspect in the second research question, we have not been able to identify any literature that covers this aspect. There is a plethora of technical and non-technical countermeasures available for both the social media platform, as well as organizations, but we would argue that the individual responsibility should be equally emphasized, hence our desire to research this.

2.6 Conceptual Framework

To best structure our research project, starting from the planning phase following every step throughout the analysis and reporting the findings, the use of a framework is highly advised to strengthen the validity and overall process of the research (Grant & Osanloo, 2015, p. 16). Grant and Osanloo (2015) argue that the analogy of the blueprint of a house, could be considered with the use of a theoretical- or conceptual framework to aid in structuring a thesis (p. 12). Just like how the blueprint of a house lays the foundation and dictates the overall scheme of construction, a framework could largely be considered an equal to this (p. 12–13). They describe further that a research plan, often in addition to a framework, strengthen the study and ensures an organized flow between the chapters (p. 13).

Grant and Osanloo (2015) explain the differentiation between a theoretical- and conceptual framework as theoretical frameworks derive from one or multiple existing theories, whereas conceptual frameworks is usually an interpretation from other researchers that includes "best practice"-variables and categories within a certain domain (p. 16–17).

2.6.1 Cybersecurity Culture Framework

In a previous small-scale pilot research project, we made use of the Cybersecurity Culture Framework as our conceptual framework. Even though this framework, from Gioulekas et al. (2022), is tailored more specifically to cybersecurity culture in particular, we have identified that several of the concepts are also applicable in this research project. The framework is presented in figure 2.1 below.

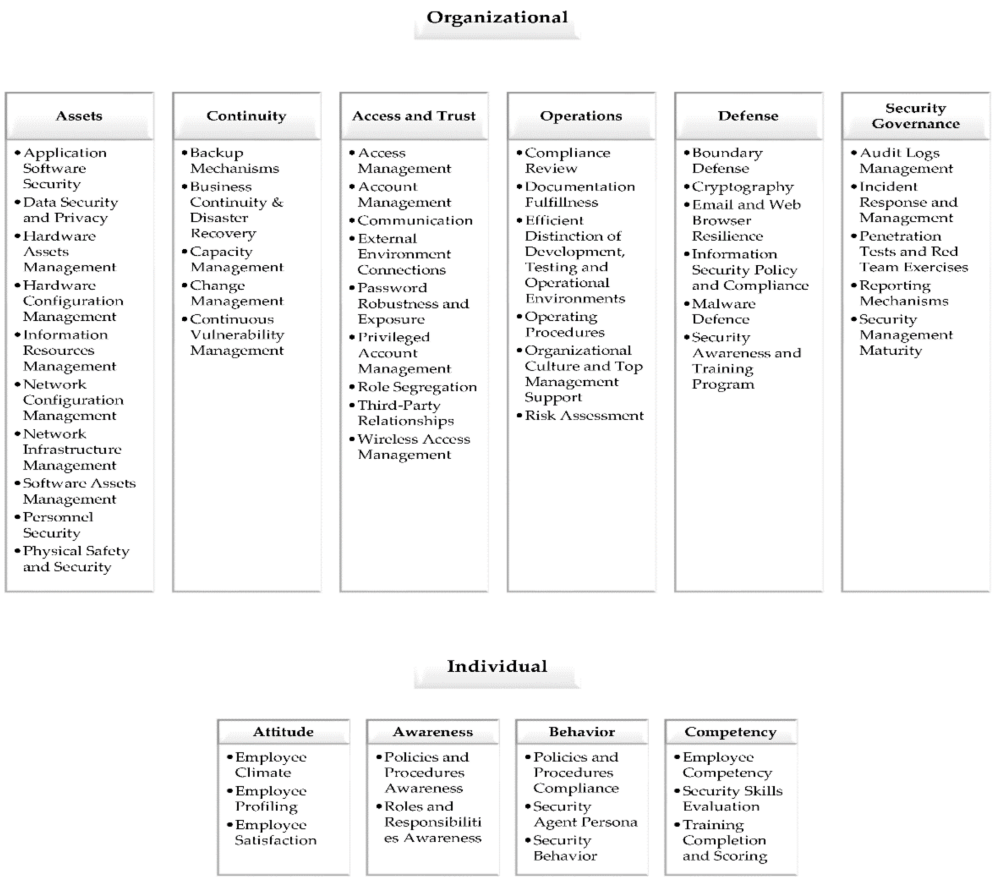


Figure 2.1: Figurative representation of the Cybersecurity Culture Framework (Gioulekas et al., 2022)

2.6.2 Our Model

With figure 2.1 representing the complete framework, we have identified that we will make use of 17 concepts within the framework. In an attempt to determine the actual meaning and description for each concept in the original framework, we found that Gioulekas et al. (2022) referred to Georgiadou et al. (2022) for their detailed description of each concept on the same framework. Through reading and evaluating each concept description, we determined which concepts we deemed fit for our envisioned aim for the research project.

In comparison to the original framework in figure 2.1, we have excluded three of the main categories, which are *Assets*, *Continuity*, and *Attitude*. With the *Assets* and *Continuity*-categories being mostly focused on physical measures and assets, in addition to overall business management, rather than our organizational focus being employees, are the main reasons as to why we have excluded these categories. Furthermore, with our focus on the individual aspect being what private users of social media should engage in security-wise, we deemed the *Attitude*-category unfit for this purpose, as this category focuses on the employee climate and satisfaction in organizations.

To help visualize our framework as best as possible, we have dissected the original framework and extracted the relevant concepts into a separate model, which is presented in the figure 2.2.

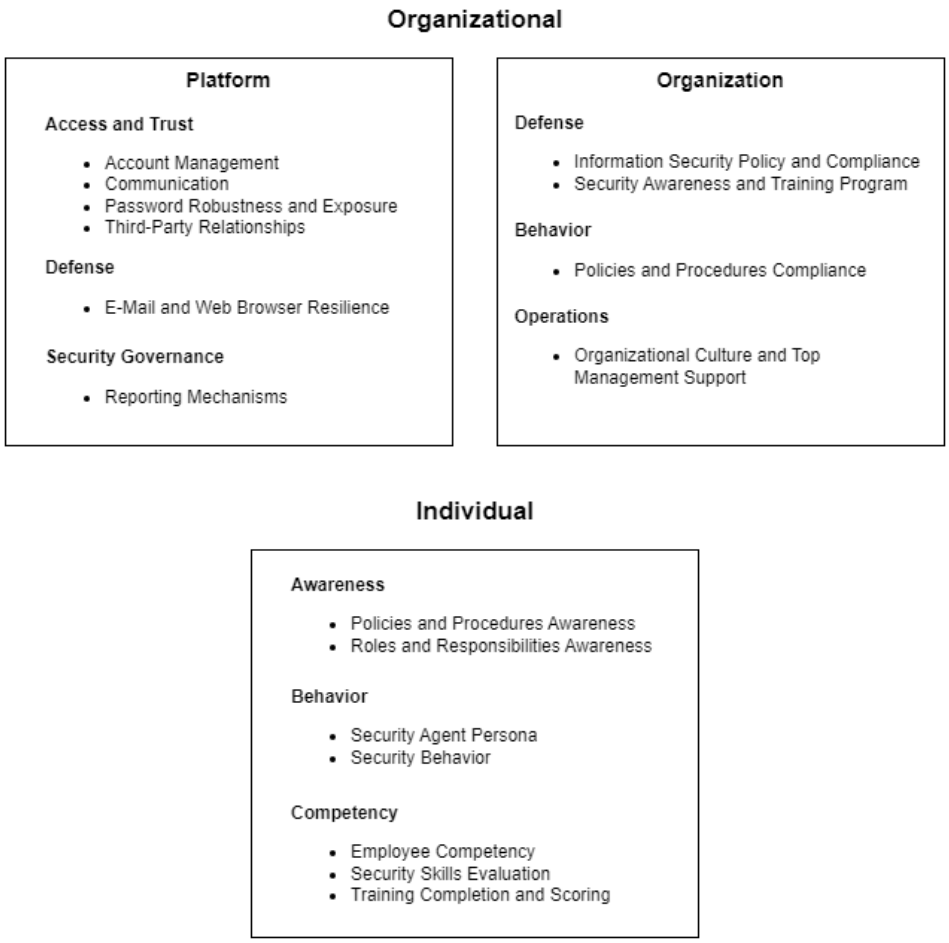


Figure 2.2: Our conceptual framework based on Gioulekas et al. (2022)'s Cybersecurity Culture Framework

In line with our three research questions, we have split the framework into three main sections, with them being *Platform*, *Individual*, and *Organization*. In the *Platform*-box, we dig deeper into what the platforms could possibly do to mitigate risks and what mechanisms that could be implemented from their side (RQ1). The *Individual*-aspect of the framework highlights the measures and concepts associated with what an individual have to familiarize him- or herself with, when it comes to awareness and knowledge of both existing potential risks and what an individual could to do mitigate the matter (RQ2). Finally, *Organization*, aims to describe what an organization could do in order to raise the level of awareness and knowledge of their employees, in addition to the policies and procedures on the subject. The importance of addressing this topic derives from the fact that employees could pose a risk to the organizations through their social media behavior (RQ3).

2.7 Related Work

In search of related work in relation to our research, we have found that Algarni and Xu (2013) have a somewhat similar approach as us, with the emphasis on how social engineers perform their attacks against users on *Social Networking Sites (SNS)* (p. 456–462). They describe the social engineers' method of approach through a *phase-based* and a *source-based* model, where the phase-based method is used to analyze the different phases of a social engineer's approach to carry out an attack, as shown in figure 2.3.

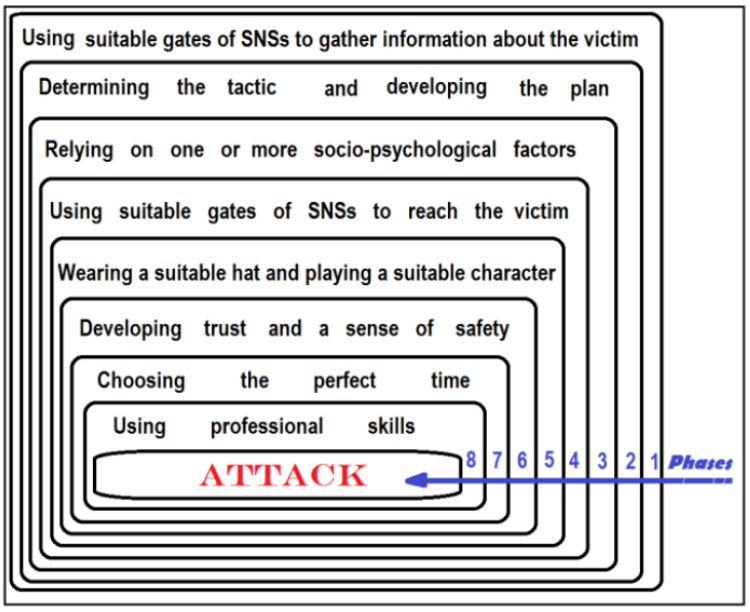


Figure 2.3: Phase-based model of Social Engineering attacks in SNSs (Algarni & Xu, 2013, p. 458)

The other method of approach that Algarni and Xu (2013) refer to is the source-based model (p. 650). Based on the first and fourth phase in the phase-based model in figure 2.3, where there are several gates for an social engineer to take advantage of for information gathering and connecting with the victim, these gates are described and explained in more detail in this source-based model (Algarni & Xu, 2013, p. 649). This figure is shown in figure 2.4 below.

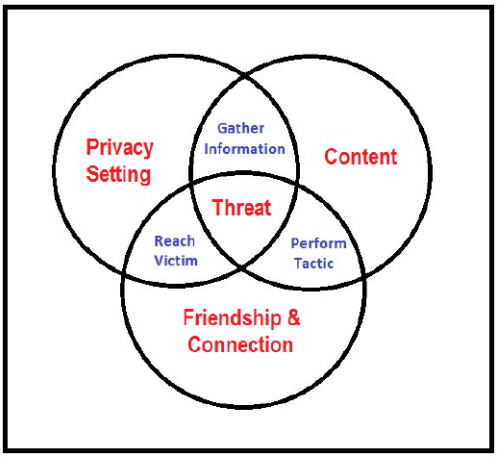


Figure 2.4: Source-based model of Social Engineering attacks in SNSs (Algarni & Xu, 2013, p. 650)

Where our research differ from Algarni and Xu (2013)'s work is that we investigate what technologies and measures that exist to secure users from the defender side, rather than having the approach of an social engineer. In addition to this, we also want to highlight how organizations could best educate their employees in safe use of social media, in an attempt to mitigate the risk of a social engineering attack on social media.

2.8 Limitations and Assumptions Based On The Literature

The aim for this closing section of the *Background and Related Work*-chapter is to provide our limitations and assumptions that we have made, based on the literature. The research areas and other subjects, such as *Social Engineering* and *Social Media*, are large and comprehensive, thus our decision to scope the larger areas to define more clearly where our attention will be focused.

2.8.1 Social Engineering

As described in section 2.1, this term encompasses several aspects in the realm of cybersecurity. On this note however, we base our definition of social engineering on Wang et al. (2020), where we see social engineering as an attack type to which attackers exploit human vulnerabilities and trust to deceive individuals to provide them with or gaining access to sensitive information through either physical or digital interactions (p. 85105).

Even though this definition is quite broad, we did not want to scope it further with the focus on one single attack method, for instance, we believe that a smaller scope would result in a case study, contradictory to our aim of the study, which is to get a holistic view of how social engineering could be used in a setting and environment of social media.

2.8.2 Social Media

With the different definitions and the lack of a common consensus on the subject of what social media actually entails, as highlighted in section 2.2, we see the need to define what social media is for our research. The aim is not to provide a separate definition of social media, rather encompassing which definitions we associate social media with, as well as which types of social media we will explore for our research.

As briefly mentioned in section 2.2, Aichner et al. (2021) have conducted a thorough review of the change in definition of social media over the years (p. 215–222). In this study, we have made the decision to adopt two separate definitions that we would argue fit well both for our interpretation of the term, in addition to how they fit into our research.

> *I) [...] we define "social-media" as Web sites and technological applications that allow its users to share content and/or to participate in social networking (Leyrer-Jackson & Wilson, 2018)*

> *II) [...] we define social media as any online resource that is designed to facilitate engagement between individuals (Bishop, 2019)*

These two definitions from Leyrer-Jackson and Wilson (2018) & Bishop (2019), respectively, both address the aspects of bonding and networking over social media, but we argue that Bishop (2019)'s addition of *"engagement between individuals"* added to the definition of Leyrer-Jackson and Wilson (2018) for the better, in regard to our research.

Lastly, as there are a number of different social media platforms available, we have decided to focus mainly on *Facebook*, *X* (formerly Twitter) and *LinkedIn* as our social media platforms of choice. Even though we have this selection of platforms that would be focused on in the interviews - if the respondents were to suggest possible topics related to other similar platforms, we would not exclude these statements, but consider them if we were to encounter this situation.

Chapter 3

Methodology

In this chapter, we cover the methods and procedures which have been used in this research project. The first of two main methods is a systematic literature review (SLR) process, which was the basis for conducting the literature review and identifying research gaps, as described in chapter 2. The second main method is a qualitative research approach, in order to collect and analyze the empirical data, which is presented in chapter 4.

3.1 Systematic Literature Review (SLR)

Webster and Watson (2002)'s title *"Analysing the Past to Prepare for the Future"* is quite a descriptive summary of what the realm of literature review encompasses. The aim is to uncover what other researchers have been investigating in the past, as well as reporting and highlighting this to further build your own study (Webster & Watson, 2002, p. 93).

Other researchers, such as Templier and Pare (2015) and Rowe (2014), have constructed, what they refer to as, a general procedure (Templier & Pare, 2015, p. 116) and a set of tasks (Rowe, 2014, p. 246), that point out the key aspects to the process of a literature review. Even though these processes are considered to be different from one another, they still are based on somewhat the same concepts, but with different wording, such as "Formulating the problem" (Templier & Pare, 2015, p. 116) and "Selecting a research question" (Rowe, 2014, p. 246).

3.1.1 Method

To carry out our SLR, we have decided to follow Xiao and Watson (2019)'s guidelines for conducting SLRs (p. 93–112). The reason as to why we have opted for these guidelines, in particular, instead of the aforementioned alternatives in the previous paragraph, is due to its streamlined process, which is easy to follow. This process is illustrated in the figurative overview (figure 3.1) from Xiao and Watson (2019) (p. 103).

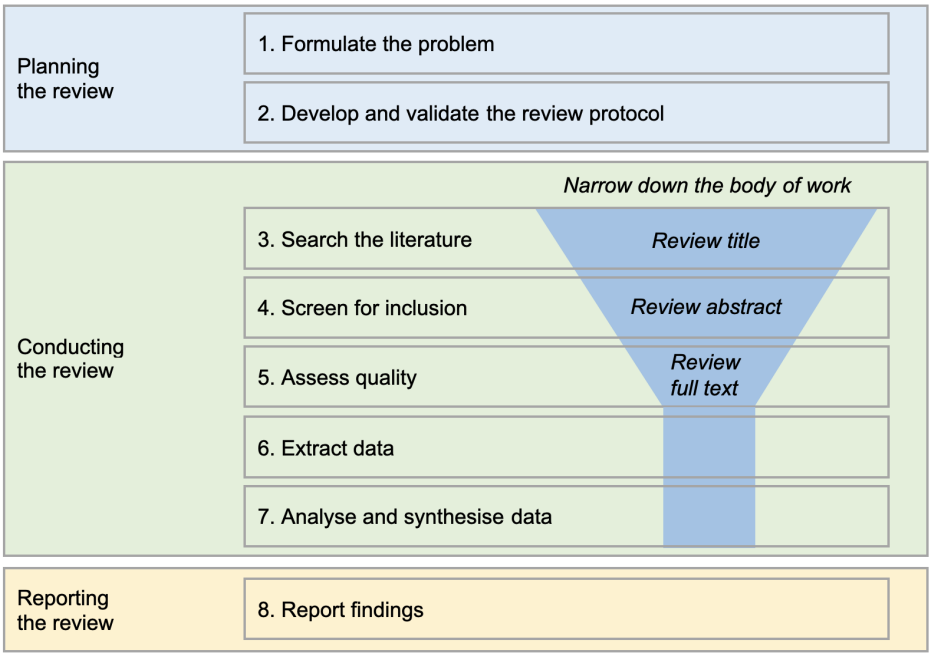


Figure 3.1: The systematic literature review process (Xiao & Watson, 2019, p. 103)

3.1.2 Review Protocol

A review protocol can often be seen as the blueprint for how you are conducting your literature review, in comparison to a research design in social science studies (Xiao & Watson, 2019, p. 103). According to Xiao and Watson (2019), the review protocol should include and describe the following elements of the literature study: *Purpose of the study*, *research questions*, *inclusion criteria*, *search strategies*, *quality assessment and screening procedures*, and *strategies for data extraction, synthesis and extraction* (p. 103). The purpose of the study and research questions are covered in section 1.

Inclusion Criterion

The research questions should be the basis for developing inclusion criterion for the literature review (Xiao & Watson, 2019, p. 105). These criterion act as guidelines for the researchers when selecting literature for the review - any irrelevant literature can be excluded based on the inclusion criteria (Xiao & Watson, 2019, p. 105). Our inclusion criterion consists of the following:

- It must be written in either English or Norwegian
- It must be relevant to our topic or sub-topics related to social engineering or social media
- The literature must have been cited at least once
- Literature must be accessible to everyone, or accessible through the university

3.1.3 Literature Search

The literature study is heavily reliant on the literature you find. A lack of dedication to the literature review, can often result in your review not being up the the required standards (Xiao & Watson, 2019, p. 103). According to Xiao and Watson (2019) there are three major methods of collecting literature being, through electronic databases, forward- and backward search (p. 103). In this literature review, we have aimed to use all three of these methods, and we will in the coming section describe how each of the methods have been utilized.

Keywords
Cybersecurity - Awareness - Defense in depth
Social engineering - Definition - History - Phishing
Social media - Definition - Sentiment analysis - Fake accounts - Machine learning - Web 2.0

Figure 3.2: Overview of keywords used in SLR

Electronic Databases

Searching through multiple different reputable electronic databases has been our main methods of collecting literature. We have tested multiple electronic databases, and ended up using *Web of Science* as our main database, as well as *ProQuest* and *Scopus* as supplementary databases. We have used multiple search words, which can be seen in table 3.2, to search for relevant literature. Most of the articles, included in section 2, have been found using the three main keywords, *Cybersecurity*, *Social engineering*, and *Social media*, in some combination. Along with these three main keywords, we have used other supplementary search words, to further narrow down the searches, where this has been necessary. From the results, we picked out each article which had an interesting title, to include for further screening and assessment.

Backward Search

Backward searches are applied to find relevant research cited in the already identified articles (Xiao & Watson, 2019, p. 104). We have through the SLR process conducted backward searches on multiple of the articles found during our search of the electronic databases. The backward searches we have conducted have yielded seven articles, which have been included for further use.

Forward Search

When conducting a forward search, researchers look through all of the already reviewed articles, looking for new articles which have cited these (Xiao & Watson, 2019, p. 104). We have attempted to perform forward searches during the literature review, without it yielding any extra articles to include.

3.1.4 Screen For Inclusion

During the literature search, the need for further screening, in order to decide which articles are suited for further inclusion is imperative, to ensure the relevancy of the articles (Xiao & Watson, 2019, p. 105). Xiao and Watson (2019) propose an efficient two-step process to review the literature, where researchers start with reviewing the abstract of the article and comparing it to their inclusion criteria (p. 105). Every article we have picked out based on the title have been review based on the abstract, prior to further analysis.

3.1.5 Quality Assessment

The last stage of the two-step process is to review the quality of the literature, which is done by performing a full-text review (Xiao & Watson, 2019, p. 106). Before including the articles for our final analysis and data extraction, we have read through each article, and excluded those who did not fit this research project. The entire process of the literature review have been summarized, and can be seen in figure 3.3.

3.1.6 Literature Search Result

To wrap up the SLR-process, we provide figure 3.3 consisting of the number of articles at different stages in the process. The bottom left box represents the net total of articles that was included in section 2.

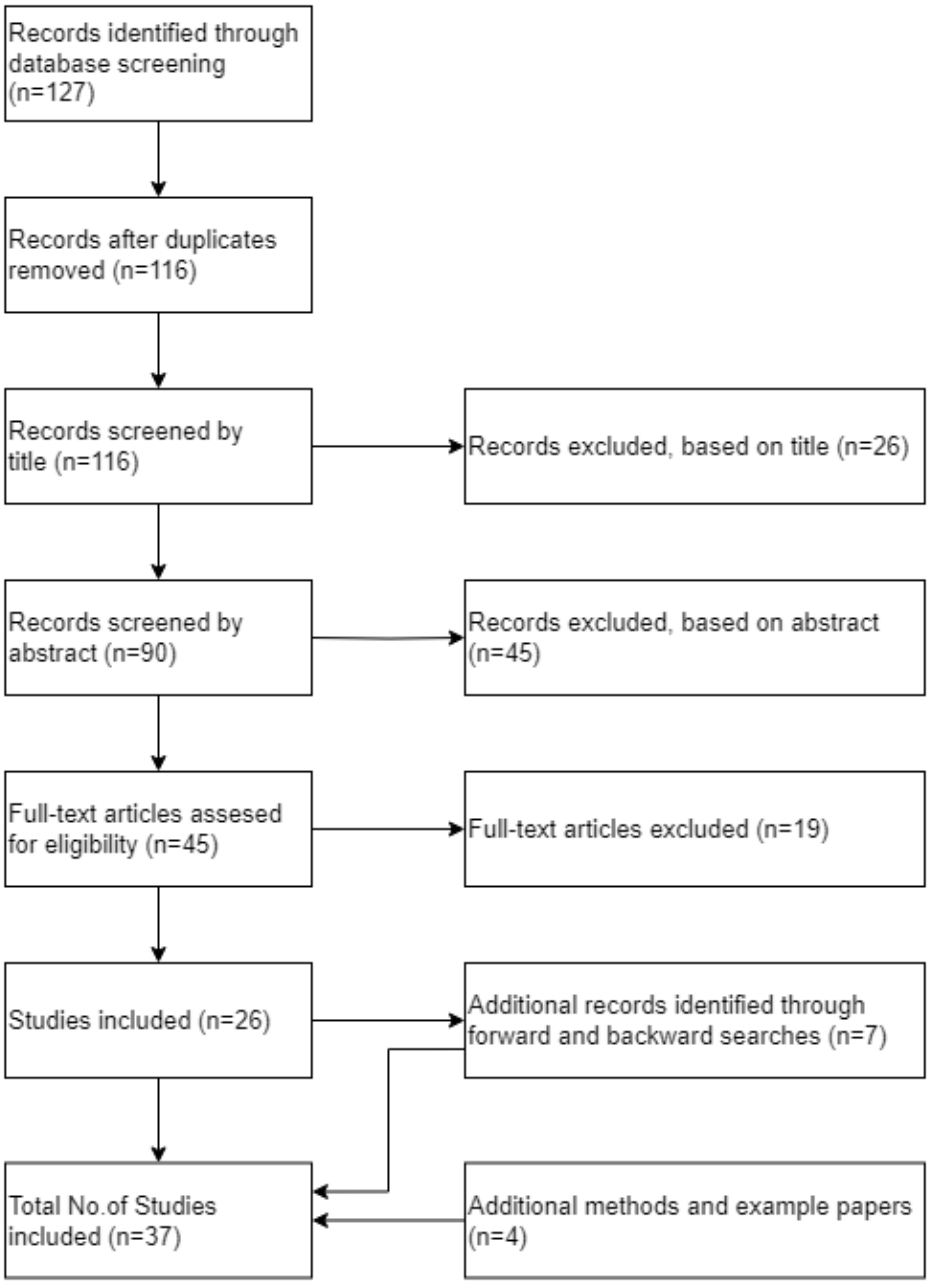


Figure 3.3: Overview of the literature search result

3.2 Research Approach

Following the chosen literature study, described in the previous section, we will now provide an overview of how we have structured our research project and a description of the employed research approach.

3.2.1 Qualitative Approach

When it comes to the differences between the two main approaches of research, quantitative and qualitative, we have opted to use Bryman (2016)'s rule of thumb, which he describes as the first approach summing up the results with numbers, whereas the other one makes use of words for this purpose, respectively (p. 375). Qualitative research is better suited for phenomenon that does not have any specific boundaries or apparent ties to their context (Recker, 2021, p. 114). Opposed to quantitative research, where the general aim could

be described as retrieving quantifiable data to test the assumptions and hypotheses, before generalizing the findings, a qualitative research emphasizes every observation, statement and any unique finding, and does not generalize these findings to camouflage them as part of a statistic (Recker, 2021, p. 114).

We would argue that these differences described by Bryman (2016), aligned with our initial ideas from the start of this research project, where we did not want to generalize our findings and quantify them - on the contrary, emphasize every finding in an attempt to answer or provide possible solutions to the research area.

In the following section, we determine and justify the choice of research approach, not only by Bryman (2016)'s rule of thumb, rather a more detailed description of the differences.

3.2.2 Rationale For The Qualitative Approach

Bryman (2016) provides a table (3.1) that summarizes some of the key contrasts between quantitative- and qualitative research (p. 401).

	Quantitative	**Qualitative**
1	Numbers	Words
2	Point of view of researcher	Points of view of respondents
3	Researcher distant	Researcher close
4	Theory testing	Theory emergent
5	Static	Process
6	Structured	Unstructured
7	Generalization	Contextual understanding
8	Hard, reliable data	Rich, deep data
9	Macro	Micro
10	Behaviour	Meaning
11	Artificial settings	Natural settings

Table 3.1: Overview of the key aspects in "Some contrasts between quantitative and qualitative research" (Adapted from (Bryman, 2016, p. 401))

When outlining our study's objective to how and what we aim to achieve during this period, based on table 3.1, we aim to describe our findings and results with words (1). We aim to get insight regarding the topic from the respondents' point of view, ideally without guiding them towards a desired answer from our part (2). With the inclusion of semi-structured interviews (6), along with us being the interviewers, we are more likely to build some kind of a relationship to the respondents (Bryman, 2016, p. 401), which effectively makes us closer to the respondents (3), unlike by the use of questionnaires, where these kinds of studies usually sends out a pre-made questionnaire with little to no contact between the respondents and the researchers outside of the invitation of participation.

Bryman (2016) describes that *Theory testing* refers to quantitative researchers that employs a framework and other concepts to base their research on, whereas theory, more often than not, emerges from qualitative research; that is at least the purpose of it (p. 401). We would argue that we adopt aspects of both quantitative- and qualitative, as we base our research project on a framework, but also the inclusion of new emerging concepts (4). For the fifth measure, *Static* and *Process*, we are somewhere in the middle of them, with *Static* referring to the depiction of a static image of the social reality, where the dependencies and relationships amongst the variables are emphasized, whereas *Process* depicts events over time along with the respondents' interactions in social settings (5) (Bryman, 2016, p. 401).

Bryman (2016) synonymizes quantitative- and qualitative research as *Generalization* and *Contextual understanding*, respectively (p. 401). Where quantitative research aim to generalize and quantify all findings, the qualitative approach aims to get a better understanding of behavior, values, beliefs and other similar concepts (p. 401). The aim for this research project fits best with the description of qualitative research, where the emphasis on a more comprehensive understanding is desired (7).

By the use of interviews, the level of richness and understanding of the data you are able to retrieve from the respondents, are typically better suited to gain a contextual understanding, along with the presence of the researcher throughout the interview would often result in richer data (8) (Bryman, 2016, p. 401). With a relatively small amount of respondents, we would not be able to draw any universal trends or conclusions, but a more focused small-scale aspect of the topic (9) (Bryman, 2016, p. 401).

In qualitative research, the aim is often to gain better insight into the rationale and actual meaning behind the topics, through in-depth analysis of the individuals, rather than only collecting opinions without context (Bryman, 2016, p. 401). Lastly, "normal" human interaction sets the standard for natural settings, rather than artificial settings, which usually entails the use of a PC or other constrained environments to answer a questionnaire, for instance (11) (Bryman, 2016, p. 401).

With the descriptions of the key aspects between quantitative- and qualitative research as a foundation, it became more clear how we wanted to structure our project. Due to the nature of our research questions, with them being more exploratory and requiring a contextual understanding to best analyze this research area, along with our desire to gain more in-depth and rich data through direct human connections, we have opted for a qualitative approach. We do believe that it could be possible to structure this research project as both a qualitative- and quantitative study, but we would argue that a qualitative approach explores the possibilities to a better degree, in addition to it aligning with what we aim to achieve through this research project.

3.3 Intellectual Reasoning

When conducting a research project, Recker (2021) provides an explanation as to how the inclusion of a plan that describes your approach for collecting, measuring and analyzing the data, and how that will tie to the research question(s) (p. 39–47). This further builds into the three main methods of intellectual reasoning, which are *induction*, *deduction*, and *abduction* (Recker, 2021, p. 39).

The purpose of defining the type of intellectual thinking comes down to what conclusions and outcome the researcher aims to provide from the research project (Recker, 2021, p. 40). As described in the previous section, regarding qualitative research approach, our aim is to emphasize all important findings through our interviews, and not generalize the results for them to merely be a part of a statistic.

Recker (2021) describes that deduction refers to basing your research on known theory and the efforts of connecting the known theory and your observations (p. 41). He refers to induction-based reasoning as drawing general conclusions from a set of observations, most commonly with an aim to formulate "new" theory from the research (p. 40). As a generalized difference, Recker (2021) further categorizes induction and deduction as *exploration* and *validation*, respectively (p. 43). On one hand, we approach our research with delving into the literature to both support and reference our findings from the interviews, which corresponds

with the *validation* approach (deduction). On the other hand, we are also susceptible for the theory and practice to contradict one another, which is where the elements of *exploration* (induction) have the potential of being introduced, based on the findings through our interviews.

In short, looking at the differences between the intellectual reasoning methods, we would categorize our aim of the project as mainly deduction-based, but with elements of induction, more specifically an inductive conceptual framework (figure 5.1), in addition to supporting articles on the emerging concepts from chapter 4.

3.4 Research Design

As referred to in the previous section, 3.3, Recker (2021) describes the emphasis on a plan for conducting research (p. 39-47). When choosing a research design, which essentially is the basis for a methodological plan for the research, Recker (2021) includes an overview with the key elements to consider into your research design (figure 3.4).

Spectrum	One end of continuum		Other end of continuum
Aim	Exploratory	vs.	Explanatory
Method	Qualitative	vs.	Quantitative
Boundary	Case	vs.	Statistical
Setting	Field	vs.	Laboratory
Timing	Cross-sectional	vs.	Longitudinal
Outcome	Descriptive	vs.	Causal
Ambition	Analysing	vs.	Designing

Figure 3.4: Research design decisions (Recker, 2021, p. 45)

Aim could be considered as the overall aim to your research, in the ranges of *exploration* and *explanation* (Recker, 2021, p. 46). We would consider our research somewhere in between them, where we want to both explore the options for securing users of social media against social engineering attacks, and try to explain what measures that are most effective to mitigate the risk, both from a technical-, individual-, and organizational perspective.

Method, as described in detail in section 3.2.2, we have opted for the qualitative approach.

Boundary tends to differentiate between case-related and statistical studies. In relation to the choice of research approach, we do not aim to summarize our findings in a statistical manner, rather emphasizing all relevant findings, without the quantification of them. At the same time, we would not categorize our research as strictly case-related, as we do not look into and make use of a case. We would argue that our research does not have any aspects of either case-related study nor a statistical lens to it, hence making this element obsolete.

Setting refers to the location the research will take place, either in the field or in a laboratory environment (Recker, 2021, p. 46). We aim to gain insight from personnel in organizations, hence our research taking place in the field.

Timing focuses on the time aspect with cross-sectional and longitudinal, where cross-sectional refers to several cases at the same point in time, whereas longitudinal focuses on the same case over a longer period (Recker, 2021, p. 46). Our research do not fit exclusively into one or the other, where we would define our research as having one case that

we got insights into from several individuals in organizations at different points in time. We did not have an overview or control over the prerequisites that the individuals have, merely their interest in participation to our research.

Outcome refers to descriptive- and casual presentation of the research area, where descriptive presentations aim to describe undiscovered phenomenon, whereas casual presentations aim to explain why the research area or the phenomenon manifest as it is known to do (Recker, 2021, p. 46). Based on these differences, we would argue that we have a mix of both, where we aim to discover something new through our research.

Ambition differentiates between analyzing and designing, with analyzing referring to investigating the root causes of a problem and designing referring to the design of a solution or an artefact (Recker, 2021, p. 46). For this research, we have chosen to analyze the topic, rather than providing a solution.

3.5 Data Collection

Based on the seven key elements from Recker (2021), we have concluded with the use of semi-structured interviews, which will be discussed in this section, along with the overall data collection phase, including respondents and the interview process.

3.5.1 Semi-Structured Interviews

With the use of interviews as part of this research project, a semi-structured approach is the most common (Recker, 2021, p. 118). A semi-structured interview usually aims to address the research topics, along with potential follow-up questions based on the answers given by the interviewee. In comparison to a structured interview, there is merely a strict set of pre-planned questions that will be asked. There is also an approach called unstructured interviews, where there is no agenda or aim for the interview, but more a conversation and creating an environment for discussion (Recker, 2021, p. 118).

Based on the explanation of the three different interview approaches, our chosen interview approach is somewhere in between structured- and semi-structured interviews. We have a pre-planned set of questions that will address the topic, basically an interview guide, which are sent to each potential interviewee for them to familiarize themselves with the topic, in addition to them having the right mindset coming into the interview. The semi-structured aspect is included by the means of the opportunity for follow-up questions, from our side, to interesting statements or sub-topics from the interviewees. The interview guide is presented in appendix A, and the consent form follows in appendix B.

With the inclusion and mix of both structured- and semi-structured aspects to the interviews, we would argue that we lean more towards a semi-structured approach. Even though we base our interview on the pre-planned questions, these questions are created in a manner that could start a discussion and does not necessarily have a concluding answer to it. Based on this, the nature of the interviews could vary largely, depending on how each interviewee express themselves.

3.5.2 Respondents

To help us answer our research questions, we have interviewed a diverse array of people, related to either cybersecurity, social media or communication. During our data collection process, we have interviewed ten individuals from different related professions, including cybersecurity consultants, senior advisors, communication advisors, researchers and experts

in the field of social media and cybersecurity. A list of the respondents can be seen in table 3.2. This group of respondents have given us a holistic view of the research problem, ensuring coverage from multiple perspectives.

Respondent	Job Title
R1	Cybersecurity Consultant
R2	Senior Advisor Social Media
R3	Security Advisor
R4	Cybersecurity and Communications Researcher
R5	Cybersecurity Expert
R6	Special Advisor Security
R7	Cybersecurity Expert
R8	Communications Expert
R9	Social Media Researcher
R10	Cybersecurity and Social Media Expert

Table 3.2: Overview of respondents and their job title

3.5.3 The Interview Process

To gather a pool of respondents, we started out by reaching out to several different organizations, both in the private- and public sector, in addition to possible respondents in our own networks. Along with the invitation, we also sent both the interview guide and consent form, providing the possible respondents a chance to familiarize themselves with both the topic and questions, as well as reading our term and conditions before the interview.

All interviews were conducted digitally using Microsoft Teams, with both of us attending each interview, leading five interviews each. The other interviewer that did not lead the interview was responsible for starting and stopping the recording, as well as the transcription in Microsoft Teams. He also took notes during the interview, and was also able to ask any follow-up questions on interesting topics.

The interview itself was divided into three parts. The first part focused on the respondent's educational level and their job position and work experience. The first part also included questions regarding their level of trust in social media platforms to protect them, as well as questions regarding the risks associated with the usage social media platforms.

The second part of the interview focused on the research problem of our master thesis - social engineering in social media, and how to this can be mitigated. The respondents were presented with questions about the use of social media in social engineering attacks, whether they think it is being used or not, along with which techniques they think are being used, and what they see as the most effective. The rest of the questions, in this second part of the interview, was tailored more towards the research questions being the responsibility of protecting users of social media, and how to mitigate the threats of social engineering in social media, from a technical-, individual-, and organizational level. As a wrap up for the second part of the interview, the respondents were asked if they had anything else to add in regards to the topic.

In the third part of the interview, we asked for feedback on the interview process itself. The recordings of the interviews were stored in a private team in Microsoft Teams, which only the owners of the master thesis had access to. When the analysis of the interviews was complete, the recordings were deleted from Microsoft Teams. The interviews varied greatly in length, with the shortest being 18 minutes, and the longest being 1 hour and 17 minutes.

3.6 Data Analysis

In qualitative research, data analysis can be seen as a way of making sense of the collected data (Recker, 2021, p. 120). During a qualitative research study, the share amount of data collected are typically massive, and knowing what parts of the data are useful and interesting can be extremely difficult (Recker, 2021, p. 120). One may use a variety of tools to analyze the data, but what is most important is the choice of analysis technique (Recker, 2021, p. 120). According to Recker (2021), there are five main analysis techniques used for analysing qualitative data, being *Coding*, *Memoing*, *Critical incident analysis*, *Content analysis*, and *Discourse analysis* (p. 120). We have chosen to use coding as our analysis technique, which we will describe further, after addressing the transcription process.

3.6.1 Transcription

All ten interviews have been recorded and transcribed automatically by Microsoft Teams during the interview itself, and we have also used a tool from the University of Oslo (UiO) called Autotekst. We found that the quality and accuracy of the transcription in Autotekst was higher than Microsoft Teams' version, hence our decision to make use of the versions from Autotekst. In general, Autotekst provided transcriptions of higher accuracy of both Norwegian- and English speaking interviews. As we have six Norwegian speaking respondents out of the group of ten, finding a tool which handled Norwegian transcription well, was important. We were recommended to use Autotekst from UiO, both from other students, as well as one of our interviewees. After each interview was transcribed by Autotekst, both of us went through the transcriptions manually, looking for and fixing any inaccuracies made by the transcription tool.

3.6.2 Coding

As previously mentioned, we have chosen to use coding as our analysis technique. According to Recker (2021), this is one of the most common techniques for analyzing qualitative data (p. 120). Coding is used to reduce the massive amounts of data, gathered during a qualitative study, into more meaningful and usable information (Recker, 2021, p. 120). Coding is also the first part in a three-step process of qualitative data analysis, called data reduction (Recker, 2021, p. 122).

During the first step of the process, we used a tool called Nvivo to code our empirical data. In Nvivo, we created categories, based on the conceptual framework and the research questions, were we could dissect each interview and extract all interesting and relevant information and statements, and map them to the relevant categories. The categorization in Nvivo made it easier to organize the information in a systematic manner, which greatly helped us when extracting the relevant information later in the process.

The second part of the three-step process is *Data Display*, where the data is extracted from the coding state into a more easily readable format (Recker, 2021, p. 122). During this stage of the process, we extracted each interesting statement and data already identified through Nvivo, and created categories to gain a better overview for further use. With the creation of categories, the statements and data were better structured, hence making it easier for us to navigate when extracting statements for inclusion in chapter 4.

The last step in this three-step process is *Conclusion-Drawing and Verification*, this is where researchers validate the gathered information with other sources of data collected during the research project (Recker, 2021, p. 122). The conclusion to our research is included in chapter 5, where we compare the empirical data, with the findings from the SLR, to address

the differences and potential contradictions between the two sets of data.

3.7 Limitations, Ethical Considerations and Potential Challenges

When conducting a small-scale research project within a tight time constraint, addressing project limitations, ethical considerations, and challenges is imperative to scope our work more precisely. This section outlines the challenges and considerations we anticipated, insights gained during interviews, the adjustments we made during the process, in addition to how these factors influenced our thesis, along with potential impact of omitted measures.

3.7.1 Challenges in Data Collection

With our research project being mainly deductive-based, as described in section 3.3, as well as adopting semi-structured interviews as our choice of data collection method, we realize that the questions we are asking in the interviews have the potential of being biased, essentially leading to an answer that we are searching for to confirm or validate our literature. Recker (2021)'s differentiation between inductive- and deductive approaches, which he describes as *exploration* and *validation*, respectively, further describes this challenge, where a *deductive* approach seeks to *validate* (p. 43). This might be considered a potential weakness to the deductive-based approach, where the aim is to validate the literature - to conduct a literature study, which then might influence what questions are being asked or in which manner they are presented, in the data collection stage.

To address this challenge, we made the decision to formulate questions in a manner that is quite open and creates the opportunity for discussion, rather than steering our respondents in a certain direction. One could argue that this is where an aspect of the inductive approach is introduced, with Recker's synonym to *inductive* being *exploration*. Recker (2021) describes that all research projects will have some kind of a combination between inductive, deductive and abductive methods in either stages of the project (p. 42). With this statement from Recker in mind, we would still argue that our research remains deduction-based, but with the introduction of some inductive methods.

Another challenge that we abruptly encountered after constructing the interview guide with the questions we planned for our interviews, was to actually recruit relevant personnel. In the planning stage of this research project, we envisioned that we wanted to interview cybersecurity personnel explicitly, to gain valuable insight into the security aspects of the relation between social engineering and social media. Our initial target group of cybersecurity personnel were hard to reach within the restricted time frame, requiring us to broaden the scope and recruit experts elsewhere. Even though we initially regarded this as a potential weakness to our study, we are quite certain that this forced alteration turned out for the better. It led us to recruiting a more diverse array of personnel, as we touched upon in section 3.5.2.

With this diverse array of personnel, we were also interested in getting their feedback on the interview process and also the dialogue, flow of communication and other actions leading up to the actual interview. This was both to unveil potential improvements that we could make as we conducted the interviews, in addition to gain a sense of understanding of our ability as interviewers. As we have not had any experience with similar research projects in the past, only a smaller-scale quantitative pilot study, we appreciated all feedback and insight into both the positives and what we could improve upon.

What we also have identified as a largely positive factor in our research project, is the fact that we have been a group consisting of two. We believe that we are able to cover

more important aspects when discussing together, rather than weighing the pros and cons individually. We will explain what we have done in practice in greater detail in the coming sections.

3.7.2 Challenges in Data Analysis

When it comes to data analysis, which essentially is analysis of the interviews, there were certain precautions and measures that we had to consider in regard to the validity and reliability of the project. It is important to highlight the measures and methods to best ensure validity and reliability regarding both the data collection and -analysis, and to be transparent about the process in which we have carried out the project.

Reliability

Grønmo (2016) describes that there is a lack of standardized methods for measuring the data reliability, but emphasizes that one could determine the reliability through evaluating the stability of the data (p. 248–249). We have made use of several steps to evaluate the stability of the data, where the first step was to synchronize the transcripts with the recording of the interviews. The way we did this was that we split the number of transcripts and recordings in half (five each). When we had finished the five, we swapped this set of transcripts and did the exact same process, only with an improved version of the transcripts to assess the quality and identify potential slip-ups or misinterpretations to the pronunciation of the respondents.

After assessing and proof-reading all of the transcripts, we used Nvivo to code and categorize the data, which is explained in section 3.6. To further assess the stability of the data, we decided that both of us coded every transcript separately before coming together and comparing the results. This process is also known as an *Intercoder reliability (ICR)*. O'Connor and Joffe (2020) describe that ICR refers to the level of agreement that different coders have on the same data, and that this ensures transparency to the process, in addition to better cover all relevant aspects of the data in question (p. 2–3).

Initially, we thought about splitting the workload in two, to make the process more efficient and get on with the analysis, but we are very satisfied with our decision to apply the ICR-method. When comparing our results, we identified some discrepancies to our two sets of coding and categorization, which might have been overlooked and then excluded entirely if we were not to use this ICR-method. Even though it was time consuming and double the workload, we would still recommend to make use of this in a group setting, regardless, to enhance the reliability of the analyzed data and the overall coding process.

Validity

The conceptual framework, presented in section 2.2, acts as a foundation for the research approach. The main reason as to why we argue that the use of a framework is important, is to ensure that there are certain guidelines, in terms of topics within the domain, that are predefined, instead of improvising relevant terms without any material to refer back to when rationalizing decisions. As touched upon in section 2.6, Grant and Osanloo (2015) compares the use of a framework in research to the blueprint of a house (p. 12). We argue that the adaptation of the Cybersecurity Culture Framework from Gioulekas et al. (2022) and its detailed description of the concepts from Georgiadou et al. (2022), increases the validity of our research through ensuring that we cover relevant topics within the domain.

With the use of the conceptual framework, we have also used this as a foundation for creating the questions that we asked the respondents in the interview. In the process of creating and

selecting questions to include in the interviews, we found it very helpful to have an array of topics for reference, while also this increasing the validity through ensuring that the questions are based on the conceptual framework. Although there are questions regarding the level of trust and the perceived risks that the respondents have regarding the topic of social engineering and social media, we have considered these questions as a segue and a means of getting the respondents started on the topic, rather than something of utmost importance to the research.

The focus area for selection and recruitment of respondents to our interviews became considerably wider than we anticipated initially, but what we believe happened for the better. In hindsight, we argue that recruiting personnel from a variety of sectors and work positions helps the researcher in gaining a more holistic view of the research area. In comparison to if the researcher were to interview a restricted set of people within the same department or whom share the same work title, that could be considered borderline niche, there are probably a smaller chance of gaining a variety of views and opinions, as they most likely discuss and share their opinions and perceptions internally, and take inspirations from each other. In relation to validity, the recruitment of personnel from several different sectors and companies, increases the external validity, instead of creating an environment of internal validity.

3.7.3 Ethical Considerations

On the note of identify potential identifiable statements or other insight that could be harmful in some way, there are also other ethical considerations that we are responsible for. With the nature of this research project being based around voluntary participation, the importance of gaining the respondents' consents was necessary. This was done through a consent form, which was also part of our application to the Norwegian Agency for Shared Services in Education and Research (SIKT). This application did not only contain the consent form to which we sent to the respondents to sign, but also an interview guide, in addition to a description of the data storage.

This consent form describes our motivations with the research projects, as well as the respondent's rights, in addition to details regarding anonymity and how we handle their personal information. The respondents were also given the possibility to withdraw their consent until May 10th 2024. Our reasoning as to why we set a deadline for withdrawal is so we would have the time and possibility to remove all of their information from every stage of the process - all the way from transcriptions to the results. The deadline for withdrawal, and our reasoning behind it, was approved by both our supervisor and SIKT.

As described in section 3.5.3, we conducted all of our interviews using Microsoft Teams. When inviting our respondents to a meeting, we made a conscious decision to not enable automatic recording of the meeting. Even though the respondents had signed on the fact that the interview was going to be recorded, we still wanted a final word of consent in the meeting before starting the recording. This was both to remind our respondents once more that everything they say and do will be recorded, in addition to ensuring that there are no technical issues before the recording starts.

Chapter 4

Empirical Findings

In this chapter, we present our empirical findings, which have been collected using semi-structured interviews with our ten respondents, as described in section 3.5. Through the use of our adaptation of the Cybersecurity Culture Framework and its categories (figure 2.1), we analyzed the transcripts and extracted the most interesting views and statements, which are presented in this chapter, through the research questions and the aforementioned conceptual framework. This chapter starts off by looking into the level of trust the respondents have in social media's capability of ensuring their security and privacy, as well as what risks they associate with the usage of social media platforms. The structure for the rest of the chapter will be based on the three research questions, addressing them accordingly. All respondents are refereed to as R and their corresponding number.

4.1 Trust and Risk Associated With Social Media

Even though the trust and risk aspects are not a part of the research questions, our rationale for including questions of these aspects is both to create a foundation and the potential to gain new insight to the overall topic that we did not consider initially. The general perception of the respondents on the level of trust by using social media can be described as low. The risks, however, are considered to be very high.

4.1.1 Trust

Addressing the level of trust, with the general perception being low, when confronted with the question, R3 abruptly answered:

> *"The short answer is no. I do not have that. Both Facebook, Twitter and LinkedIn have had data breaches in the last ten years. [...], where customer data has been lost."*

Along with R3, several of the other respondents also expressed concerns with trusting social media platforms - some just blatantly stating that they do not trust these sorts of platforms, and others had some more interesting views on the topic, more specifically an economical aspect. R5 also answered that they do not trust these platforms, but with a different reasoning than the previous statement from R3:

> *"No, I don't. I'm just thinking these companies have a purely economic interest in what they do on privacy and security. [...] the level they provide will be the level that is either mandated by regulations, and even that is questionable [...]."*

The economical aspect of this statement is very interesting, and this was further supported by R7, who do not directly mention the economical aspect, but clearly believes that these platforms will do what they need to, and what is expected from them, but nothing else:

> *"No, I do not [trust social media platforms]. I trust that they will take care of their own security beyond their own needs. And then they do what is required from them in regard to societal needs and regulations, but not more than that."*

Even though social media platforms might not do more than what they are required to, we live in a time and world where social media have become a crucial part of many peoples lives. R10 touched upon this balance in their response:

> *"We can't fully trust social media, but we need it. So that is the balance."*

The balance between trusting these platforms and the need for them can be extremely thin and hard to manage. This point is further elaborated by R9, who does not completely trust these platforms, but mentioned something which we as consumers might not think about:

> *"Not quite [trust social media platforms]. But yeah you kind of like [trusting] by using them [social media platforms] you kind of like blindly assume that you're going to be okay until you're not."*

To sum up, the respondents generally do not trust the social media platforms to ensure their privacy and security, anyhow the fact that people keep on using them, means that they trust these platforms to some extent, whether they think about it or not. The hard truth is that people need these platforms; people are progressively becoming dependent on social media in their everyday life and an absence from these platforms is not an option for most people.

4.1.2 Risk

Social media brings a lot of advantages with them, but there are various risks associated with using them, and the risks a user exposes him- or herself to through usage of social media are plentiful. R3 discussed the high risks of using social media, along with sharing their thoughts on the use of these platforms, from a penetration tester's view:

> *"I would say that it is generally quite high risks in using such platforms. [...] if I see it from a penetration tester's perspective, if you are going to attack either an organization or a person, social media is one of the first places you start to look for information."*

The risks associated with sharing personal- and sensitive information tie in to other respondents' answers, more specifically the answer given by R9:

> *"There is a risk of exposure. Everything you put out there, everything you react to can be used for or against you."*

Generally the respondents focused a lot on risks in regards to the information a user publishes on these platforms, and the consequences you might suffer from posting information on social media. Along with that, they also mentioned risks like, phishing, impersonation, consuming disinformation or misinformation, and social engineering.

When the respondents were asked whether they believe there are any differences in risks using social media for private and work, R5 gave a reflective answer:

> *"I'm tempted to say yes and no at the same time, because on the abstract level, the risk for private and for business use is entirely the same. So, there's a plethora of things that can go wrong,[...]. However, the consequences that you face differ."*

R5 further elaborated this, giving an example of how a private user might post something that only their friends will see, where an organization posting or sharing something that they should not on social media, might damage their reputation or market. These comments from R5 are mostly in line with other responses given by the other respondents, with them also stating that the risks might be the same, but that the consequences differ.

4.2 Platform

After getting the respondents started with questions regarding their trust in social media and the perceived risks associated with it, we move on to the main part of the interview, where we aim to address the three research questions through several sub-questions. Following our conceptual framework, the first research question builds into the *Platform*-box (see 2.2). The first research question is as follows:

RQ1: Which technologies and measures exist to help secure users of social media platforms from social engineering attacks?

Several key themes have become central throughout the analysis of RQ1. The first one is *Technical Possibilities*, which entails technologies and measures that can be implemented from the platforms. Secondly, *Artificial Intelligence*, addresses how AI and machine learning can aid in mitigation of social engineering. *Implemented Platform Security and Economic Interests* refers to regulations, obligations, and economic aspects. Lastly, the *Interrelation between Technical- and Human Aspects*, in relation to implementing measures of technical and non-technical sort.

4.2.1 Technical Possibilities

In regard to the technical possibilities, several of the respondents stressed the need for certain password requirements, encouraging the use of a password manager, various multi-factor authentication options, and enabling login alerts that directly tie to the users of social media. R2, amongst others, discussed the topic of filtering and safe-listing, where R2 reflected on the internal browsers that several social media platforms have integrated:

> *"If you click [on a link] in the platform, it will render an internal browser in the application. It is obvious that you might gain access to something that might not be good. [...] The first thing that comes into my mind is that the filters have to work well, and maybe some kind of sealing, safe listing of domains. I don't know how this would work in practice. It could potentially be an exclusion machine that would receive a lot of critique."*

Even though R2 reflected on this suggestion that it may be an exclusion machine, meaning it could result in excluding legit and non-malicious websites. It could still be a possibility to limit the access or filter certain domains, especially of which are illegal or damaging in some way.

Several respondents discussed a huge risk when using and being engaged with social media - fake accounts. This is usually a profile where the social engineers hide behind, and could be either compromised accounts of victims, or fictive accounts with some compromised information to make this account seem more legit. The topic of unique identification, in relation to the creation of fake accounts, is brought up explicitly by R2:

> *"Regarding setting up accounts - I wouldn't want to sign on with BankID when I'm logging in to Meta myself, but I'm sure that this type of hard [unique] identification could solve some issues."*

With BankID being a unique *national* identification method in Norway that the majority of the Norwegian residents utilize to for authentication reasons, in addition to enter banking and other sensitive public services, R7 discussed other methods of identification that does not tie to your personal identity:

> *"[...] there have also been some variants of verified accounts and such, but they usually charge you for this, and then it is only companies that would choose to pay for such features. Companies and celebrities, politicians and such."*

This type of verification is not considered as unique identification, where unique identification calls for personal information, such as social security number or similar uniquely identifiable to your individual. There are similar verification features on LinkedIn and Instagram, where you can get a verification badge on your profile if you fulfill certain criterion.

4.2.2 Artificial Intelligence (AI)

The use of AI, and its potential pros and cons, is brought up as part of the technical measures from the social media platform's side. The areas of application ranges from filtering, as touched upon in the previous section, to performing sentiment analysis and behavioral analysis of the users of the different platforms. On the other hand, the concern for AI-generated content is also mentioned, along with the potential use of AI as an assistant for attackers. R10 summed it up as:

> *"[...] AI for attacking and AI for generating malicious content or AI for protecting."*

R9 discussed an analogy in relation to AI, which also further builds to the statement of R10:

> *"Like everything, it [AI] kind of depends on how it is used and how it is designed and for which purpose. The problem with security [and AI] is that it is indeed a blade like a double [edged] sword. [...] Because [...] what can be used for good can also be used for the wrong purposes. As long as artificial intelligence is supervised it is used as an assistant to the human component [then it could be possible]."*

Other respondents are doubtful whether the development of AI is advanced enough, at this point in time, for it to being able to be part of any solution or mitigation for social media platforms. What some respondents do believe AI is capable of today, in relation to social media, is to analyze the behavior of certain groups and the emotional tone of texts and posts on the social media platforms to try and predict or interpret potential harmful actions to come, in other words - sentiment analysis.

4.2.3 Implemented Platform Security and Economics Interests

Several of the respondents highlighted that all technical aspects should not necessarily require the user to make a conscious action in order to use it, rather it being part of the social media platform's back-end mechanisms. R7, in particular, presented a technical aspect in this regard:

> *"[...] to some degree maybe there should be some kind of a mechanism to delay the response."*

R7 referred to the delay response as a platform measure to implement an opportunity to withdraw or modify actions related to information sharing, such as posts one may regret publishing. R8 had a slightly different angle of approach to the "delay response"-aspect:

> *"[...] it could be that the government should implement a delay on some of these transactions [transactions: in relation to posting, submitting or sending content on social media]."*

R7 and R8 made the same point, only with R8 believing that the motivation should originate from the government or through a similar legal instance. Contradictory to the approach that R8 has, R5 described how they perceive the social media platforms view any legal obligations (same statement as in 4.1.1):

> *"I'm just thinking these companies have a purely economic interest in what they do on privacy and security. [...] the level they provide will be the level that is either mandated by regulations, and even that is questionable, whether they would always go for that or the levels that they deem necessary in order to keep users hooked up. [...] But for simple economic reasons, the level will be kept as low as possible."*

R7 shared a similar opinion to R5's statement:

> *"[...] if you look at the likes of [Mark] Zuckerberg, do you think that guy gives in [to the legal obligations] if he is told to do this and that? Don't you think that he will do anything in his power to find a way around it? [This is] because the entire business model bases itself on data harvesting."*

Both R5 and R7 referred to the business model and the economic interests that are present in the social media platforms. R7, in particular, further discussed their doubts when it comes to focusing on user-related security and if they were to consider implementing such, they would see a clear economic reward to it. To support this opinion, R7 contextualized it with:

> *"[...] let us say that they force [the use of] two-factor [authentication], and 10 % of your users are not able to make two-factor [authentication] work, then you have lost 10 % of your customers. Not necessarily that they have resigned from the platform, but if they are not active [users], you generate less money."*

R7 further discussed that there will always be a cost-benefit analysis when it comes to implementing, and especially forcing, additional features, and when the platforms themselves do not necessarily capitalize on it, then why should they force it through?

4.2.4 Interrelation between Technical and Human Aspects

When confronted with the question of what the social media platforms could do on a technical level, R9 responded with:

> *"[. . .] on a technical [level] it's kind of weird because you can have the most technical, the most advanced security controls and all that, but without the social aspect or like that contextual aspect of it is, you can have everything [and still fail]."*

Even though this does not answer our question directly, it showcases the ever-important need for focusing on individuals, equally as much as the technical aspects. R1 had a statement that correlates to this one, being:

> *"[...] there are various things that could be done on the technical side, but I don't think that you will solve it 100% through the technical [aspects] [...]"*

The two statements, questioning whether technical measures and mechanisms are enough to mitigate the risk of falling victim to social engineering attacks, builds into the human aspect of the matter. Without any emphasis on the education or enlightenment of the users to be aware of certain red flags to be on the lookout for, there are no technical measures that can prevent this.

4.3 Individual

With the two last statements in the previous section concerning the human aspect, this acts as a segue into the second research question. It has almost become a cliché in the cybersecurity domain that you can have the most advanced systems, but if the users do not comply and are aware of the risks from attackers, all it takes is one click on a malicious link or attachment, and the attacker is in.

To address this human aspect, the concepts within the *Individual*-box in our conceptual framework, figure 2.2, act as a basis for this research question.

RQ2: What responsibilities lie on the users of social media platforms to protect themselves against social engineering attacks?

Throughout the analysis of RQ2, several themes have arisen. Mainly, the *Responsibility* of the individuals, which the research question also calls for. Furthermore, addressing *What Users Should Actually Do* in terms of securing themselves on social media, in addition to the *Education and Awareness of Children.*

4.3.1 Responsibility

The questions of responsibility among the users of social media platforms resulted in most respondents discussing the balance between the user's responsibility and the platform's responsibility. In some aspects they may overlap each other, causing discussions and a variety of answers. Starting with the user's responsibility, R9 opened with:

> *"I feel like as a user your responsibility starts when you sign up for a social media platform. And that's where you start in your signing up to the pretty much, I call it [...] "you're making a deal with the devil". Because you're signing up for*

your data to be used at their like at the convenience of a social media platform."

The message of this statement can be reduced to that you should be aware that your data will essentially not be your data anymore, and you should consider if you are willing to risk it, in addition to be cautious of what you are sharing at these platforms. R2 shared a similar view on the topic:

> *"In principle, I think it is my job to secure my own accounts. If I am not able to do it, I should not have a presence there. [...] but we also have to realistically look at what people are capable of - not everyone will be super users of this."*

What Should the User Think Through?

To follow up the two previously mentioned statements, R8 provided a three-step thought process that could help potential users in evaluating whether they are in actual need of an account on the particular social media platform in question:

> *"So I think the first thing to think through is "do I really need this?". And "what is it that I want to achieve by signing up?". Number two, if I decide to sign up, [...] I think it is important to familiarize myself with the conditions. Number three, purely security-based, [...] what kind of security does these systems [and platforms] provide, and how do I use this security to protect myself?"*

Such a simple and logical thought process, yet universal in terms of that this could encompass, not only choice of social media platforms, but any other digital service that requires signing up and creating an account, could help potential users sorting out their thoughts and through this decide whether they want to engage in it - basically performing a cost-benefit analysis. R9 also believed that a certain degree of user awareness regarding terms and conditions could be used as a guide:

> *"Learning what the platforms do, and most importantly learning what social media networks can do with your data. Like once you find that out then you become more conscious into like what you're putting out there, and how you're interacting with these tools [platforms]."*

4.3.2 What Should Users Actually Do?

Like touched upon in the previous research question, passwords are also mentioned here. A specific solution to maintaining a secure and reliable password storage is the use of a password manager. The respondents encouraged the use of password managers where this is possible, both to being handed strong passwords and having them stored safely. If, however, you use a password manager, good password practices should be part of your routine. R2 provided a specific scenario and recommendation:

> *"Use long passwords, that was status quo last time I checked. It is not too important with all these weird symbols – they have to be long. I read something about [...] Handshake hacking. You can, on a Wi-Fi, intercept the handshake and upload this handshake to a server with immense computational power. If you have a long password, the time it takes to retrieve it is considerably longer compared to a shorter one."*

Even though handshake hacking may be more applicable for retrieving Wi-Fi-passwords, the importance of good password practices is evident. R3, on the other hand, also emphasized

password creation and good practice, but in a different way:

> *"[...] strong passwords, don't reuse your passwords. If one password is compromised, all of the sudden, all of your users are at risk."*

4.3.3 Enabling Security Controls

With most respondents discussing the responsibilities of securing accounts from a user's perspective and also concluding that it is mostly the user's responsibility to secure their own accounts, R7 contradicted most respondents by stating:

> *"[...] when I think of social media and securing accounts and such, then it is at the mercy of the [social media] platforms. Not just the technical possibilities, but also how it is shared with their users."*

On the topic of security controls, there is a discussion of who is actually responsible for them. Some respondents argued that it is the user's responsibility to activate them, while others emphasized that the platforms are responsible for both implementing them, as well as making them available and encouraging the average user to make use of it:

> *"We as individuals are probably not able to make a particular difference. We have, to some degree, the responsibility of activating the [security] mechanisms, but then again if it is not made easy for the average Joe, it is realistically not good enough. It should not be necessary to be a super-specialist [...] to achieve this [sufficient security]." -R7*

4.3.4 Education and Awareness from an Early Age

With the group of users of social media platforms ranging from children to elderly people, some respondents addressed their concerns especially regarding children consuming a lot of content from these social media platforms. With the awareness- and knowledge levels being naturally low, if not completely absent, along with the lack of critical thinking, this could have huge consequences:

> *"[...] if you were to be raised with [using] social media [on a regular basis], even before you could read or write, then it is almost baked into your identity." -R7*

When using social media platforms and sharing posts or some other type of content, maybe even personal information or controversial opinions, users may not realize the consequences of this:

> *"It is clear when it comes to the responsibility we have ourselves, that we are back to the terms of awareness and maybe not post things on these [social] medias that you don't want to lose control over. [...] but I think very few of us realize the consequence of losing control." -R7*

In an attempt to address this issue, or at least making children aware of how damaging sharing such information could be, several respondents raise the topic of introducing some kind of awareness into the school's curriculum. R5 summed up how it could work in practice:

> *"I think it's something that you probably can start [with] as early as elementary school and it probably should be something that is built on recurring events. [...]*

at the point of time where children typically will start using all mobile devices to also make that a topic in school, which of course requires teachers to be educated on that. But I think it's something that can be started with quite gently and provoking children to be more critical about what they hear, because from my own experience, they typically come up with the right answers themselves."

4.3.5 Differences in Physical and Abstract Experiences

Real-life traumatic experiences will most likely stick with one, and the consequences will also most likely be very real and maybe even physical. R8 compared social media and car driving:

> *"If I highlight it from a different angle – car driving. Then I might realize that [...] driving without brakes would be madness, but these social medias might be, in some way, more abstract maybe. We don't see the direct consequence of what we are doing."*

When using social media or any other digital service, users may not be able to see the consequences as it is not necessarily physical or directly impacting you at that point in time. Whether you are able to realize and understand the potential consequences of your actions online, R10 argued that:

> *"[...] it is like really depending on [the] individual understanding on cybersecurity."*

Even though this is not directly relevant for this second research question, the abstract perspective is important to emphasize and reflect on as individuals. Contradictory to physical interactions, where the impact is very noticeable, abstract and digital experiences are still just as important to take seriously, as the consequences faced could be evenly threatening.

4.4 Organization

This last section of the findings is tailored towards organizations and what they can do to help prevent their employees becoming victim of social engineering in social media, in addition to what responsibilities lie on organizations, and what can they could do to raise the awareness levels of their employees. We have used the *Organization*-box from our conceptual framework, figure 2.2, as a basis for this research question:

RQ3: How can organizations educate their employees in safe use of social media to reduce the occurrence of social engineering attacks?

The main themes for RQ3 are the focus on *Training and Awareness*, focusing on *Onboarding* and the emphasis on *Repetition*, including *Rules and Policies*, in addition to *Top Management* and the need for *Strategies and Clear Philosophies*.

4.4.1 Organizations and Their Employees Role

When asked about how organizations can help their employees staying safe on social media, several of our respondents started discussing the importance of an organizations employees in their work towards keeping the organization safe from cyber threats. R2 summarized it like this:

> *"I think the employees have a very important role in all cybersecurity work in an organization. Although it is more complicated than that, there is still some*

truth in the fact that the chain is no stronger than the weakest link."

Given R2's response in the light of social engineering in social media, it can be easy for organizations to think that it is a personal issue that the employees must fix themselves. The fact is that this sort of attacks can be very harmful for the organizations as well, and therefore the organizations should take this into account. R2 further discussed how better awareness and knowledge about this topic from the employee, can be of benefit for the organization:

> *"[...] It will also benefit me as an individual if my security regime gets better and more effective. It will also help my employer not to be afraid of a data breach happening because of me."*

Furthermore, R5 discussed if organizations could do anything to help combat these types of attacks:

> *"I think that organizations can both on an operational and on a strategic level take some decisions that will put in their weight towards countering social engineering, towards countering misinformation, disinformation on social media."*

4.4.2 Training and Awareness

When asked what organizations could actually do, there was a broad consensus among our respondents that starting with training and increasing the awareness level of their employees was important. One of the respondents that brought this up was R7:

> *"I think that you have to start with raising the awareness of it [social engineering in social media]. As simple as that, and maybe don't start with a scolding sermon, and don't start with admonitions and moral aspects, but just start with awareness."*

Having training and raising the awareness levels on the topic of social engineering, social media, and cybersecurity, in general, are important, which most of our respondents also agreed with. R5 suggested that training programs in organizations can, and probably should be made mandatory:

> *"[...] make mandatory training. That should be something probably to all users who will use social media, even just a consuming role for a company."*

Making training programs mandatory will make sure that all employees, regardless of position, will get some sort of training or education on safe use of social media and cybersecurity.

Onboarding

The first suggestion from the respondents was to introduce cybersecurity, and also safe use of social media when onboarding new employees in an organization. Onboarding meetings serves as a good platform to introduce new employees to core concepts and important information within an organization, as described by R2:

> *"[...] I believe that the first period after you have been employed, and the training you receive [during that time], lasts quite a long time. Because it says something about what the organization thinks is the most important to you."*

R4 further discussed the importance of having the topic of cybersecurity and social media included in the onboarding process:

> *"I think very important for new employees is onboarding meeting to provide them with information in regards to what they should do and what they shouldn't do [...], I think this onboarding could help in providing or getting everybody onto a basic understanding of what they should do and not do and how they should act,"*

On the other hand, R9 had a different opinion on including this in the onboarding process:

> *"I don't believe in that security training that people do in the onboarding of companies, like that is a bunch of like PowerPoint slides [...] but it's more like I think having conversations."*

R9 is not against having cybersecurity and social media as a part of the onboarding process necessarily, but emphasized that we can utilize different methods other than standard PowerPoint presentations and lecturing, maybe having simple conversations instead.

Risk and Consequences

In section 4.1.2, there are mentions of the risks associated with being present on social media platforms. This was further brought up in regard to what organizations can do, then in the context of making their employees aware of these risks. R2 talked about the importance of this:

> *"[...] you have to be aware that the risks exist. That is the first step, if you manage to make as many in the organization aware that there are actually some risks associated with their presence on the various [social media] platforms. Then it enables people to seek more knowledge about it."*

R3 further discussed what information the employees should be given, in regard to the risks of social media:

> *"The awareness of the risks of cyberattacks on social media must be raised as much as possible. Give employees a good overview of the potential scope of a cyber incident on social media, and give them an idea of how cybercriminals operate."*

Along with informing employees on the risks, some of the respondents also mentioned raising the awareness regarding the possible consequence of these attacks. R3, in particular, mentioned:

> *"Getting people in an organization to understand the consequences and risks, that i think can have a very good effect on building a [good] security culture. [...] You should not scare your employees either. Then you have to find the balance. That they understand the scope, but that you do not scare them."*

Finding the right balance between educating and scaring your employees can be difficult, but if an organization would be able to do that it might be a good way of raising their employees awareness levels.

Gamification

R10 brought up gamification as an alternative for educating and training employees, and people in general.

> *"I see that people finally want to learn that [cybersecurity] as a game, because you will get a score and there is a rank scoreboard"*

Taking a more "modern" approach to educating people might be a good idea. R10 further elaborated that in this day and age, more people are engaging with video games, and other sorts of digital entertainment, why not try this for education and training on cybersecurity as well.

Repetition

Along with focusing on training and raising awareness, several of the respondents brought up the need for repetition. R10 explained it like this:

> *"Organizations should understand that people forget about what you have taught. That is, you have to remind again, memory working like this. [...] Because people might forget about those things and especially also about differentiating something that is real and unreal."*

In general, people often forget what they have been taught, especially things that might not interest them a lot. Reminding people what they should and should not do is important, R4 further discussed one of the consequences of not reminding people what to do:

> *"[...] after months and even years they are probably taking the easier way to do things, and [we should be] refreshing these memories and what to do and not to do."*

The individuals that opt for the easier solution to their everyday tasks could pose a threat to the organization, if this trend is upheld. In order to remedy this, R4 mentioned the aspect of repetition in training and awareness programs:

> *"I would think that regular workshops and meetings where people get updates on new types of attacks and refresh their memory on how they can protect themselves and the company and what they should avoid [...]. "*

Cybersecurity is in constant evolution, with new threats, risks and consequences emerging. Through repetition, by the means of regular workshops and meetings to repeat the basics and core concepts, it would keep employees up to date on the possible threats they might encounter.

4.4.3 Rules and Policies

Training and education is an important and effective way of raising the awareness of employees, but there are also other measures that organizations can utilize to protect their employees and themselves from social engineering. Several of our respondents mentions the importance of having rules and policies in place. R5 described it like this:

> *"You need something like official guidelines on social media usage. So, this would be the internal guidance, and also the possibility to enforce if there's*

some wrongdoing."

Not only will these guidelines tell the employees what they can and can not do on social media, it will also make sure that the organization have something to enforce, should their employees do something wrong on social media. Organizations will not necessarily be able to *control* how their employees behave on social media on a personal level, but could have rules and policies for work-related social media usage to hopefully *affect* their behavior. R4 further discussed the possible implementation of rules and policies for social media usage like this:

> *"It could highlight that people should follow these instructions and that it is not a suggestion basically, but it is kind of mandatory that they act in that certain way not only for the company's sake, but also for the user's sake [...]."*

As R5 stated, making it mandatory to follow these rules, and highlighting the fact that it can be positive from both a company and personal level for the employees, might be beneficial for the organization. In addition to implementing rules and policies, R8 mentioned the possibility of restricting the use of social media, especially during work hours:

> *"How can we raise the awareness regarding the use of social media at work? Should it be allowed?"*

Restricting access to social media platform might bring some issues with it, but for some organization this might be an effective and necessary solution.

4.4.4 Top Management

Some of the respondents also brought up the importance of the management of an organization when it comes to raising the awareness of their employees. R7, in particular, explained it like this:

> *"The management must be made aware that this may be a good idea [focusing on cybersecurity], to have a professional relationship towards it. To increase the employees awareness, you have to start with the managements awareness."*

It was further discussed that this will differ from organizations, but that for most organizations it will be necessary to start by raising the awareness of the management, as well as the employees.

Strategy and Clear Philosophy

Along with the focus on raising the managements awareness, and making the employees acknowledge the importance of focusing on cybersecurity, the respondents also mentioned the importance of the organization having a plan and a strategy in place for the use of social media. R5 mentioned it in this manner:

> *"[...] is to set up a social media strategy. To be very clear on why you use social media and besides this purpose, what it entails for you. And to be quite clear on what you do."*

A clear strategy can be a great tool for employees that uses social media on the behalf of the organization, as well as their private presence on these platforms. R5 elaborated on this further:

> *"I think anything that you do as a kind of outreach activity should have a clear strategy behind it. So, it needs to be clear for what purpose, what are the measures, how can you control it, how can you steer it? And particular, what do you do if things go wrong?"*

Focusing on the managements awareness and knowledge, along with having a clear plan and strategy for using social media in the organization can be important parts of keeping the employees and organization safe from social engineering.

Chapter 5

Discussion

This thesis aims to understand the role of social media in social engineering, more specifically how social media as a platform is being used for conducting social engineering attacks. Along with that, this thesis also aims to look into how these types of attacks can be prevented from a technical-, individual- and organizational level. To accomplish this, we have conducted a systematic literature review to collect and analyze relevant articles and literature for this topic - these findings can be found in chapter 2. Along with the literature review, we have collected empirical data, through the use of semi-structured interviews, which is presented in chapter 4. This chapter combines the findings from both the literature review and interviews to get a broad understanding of what measures exist, and what can be done to mitigate the occurrence of social engineering through social media platforms.

5.1 Inductive Conceptual Framework (ICF)

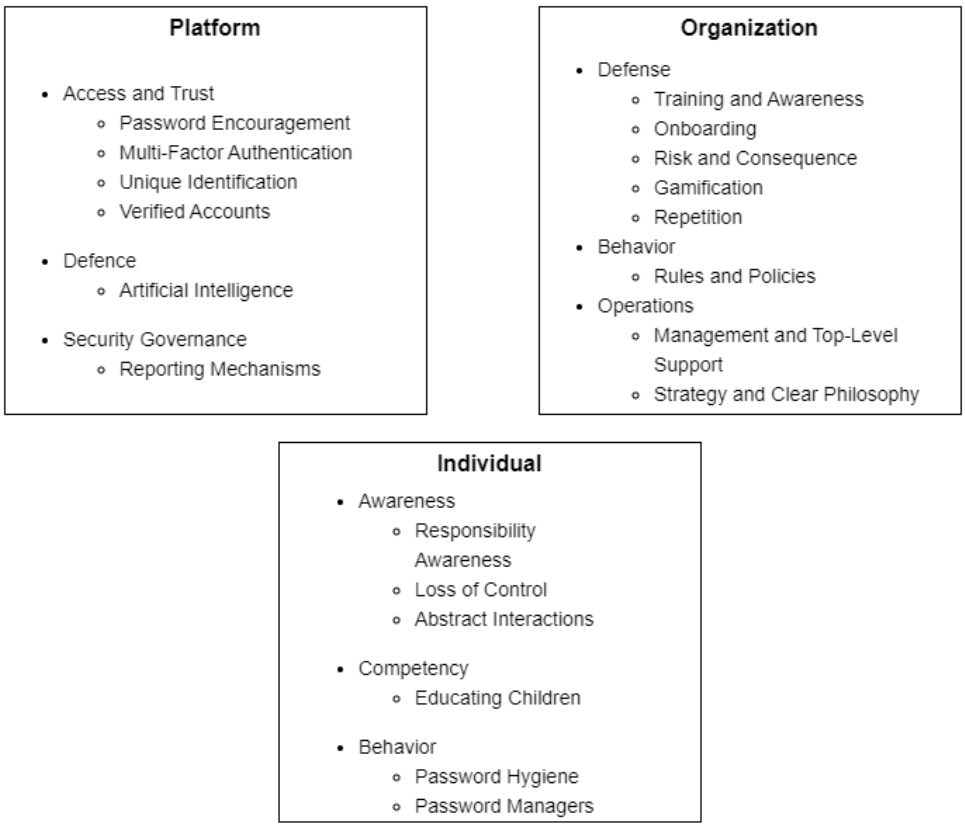


Figure 5.1: Inductive conceptual framework with categories and adherent concepts

The figure 5.1 provides the inductive conceptual framework (ICF), which is based on the conceptual framework (CF), as presented in figure 2.2, and the emerging concepts through the empirical findings. This ICF is organized into the three main sections, *Platform*, *Individual*, and *Organization*, similar to the CF. Where the ICF differs from the CF, is that the ICF offers in-depth insight into the existing categories and their concepts identified through the empirical findings.

As there are certain concepts that have emerged through the empirical findings, there are no coverage of these concepts in section 2, such as "Educating Children" and "Management and Top-Level Support". With these emerging concepts not necessarily being brand new and innovative, we have made an attempt to gather literature on these concepts to investigate the coverage of them.

The overall sections, categories, and concepts presented in the ICF (figure 5.1) will be the structure for the remainder of the discussion chapter, addressing what each concept refer to.

5.2 Platform

The first section of the discussion addresses the possibilities that the social media platforms have when it comes to help securing their users. This includes both concrete recommendations on already existing parts of account security and other measures that are theoretically possible, but that has not been implemented yet, to our knowledge. Through the interviews, respondents seemed to find it challenging to differentiate between the platform's- and user's responsibilities, as the two are closely related, where it may be the platform's responsibility to implement the certain measures, but it is up to the user to enable them. Nevertheless, the respondents provided their opinions as to how the social media platforms could do a better job in both informing and encouraging their users to make better security-related decisions.

5.2.1 Access and Trust

The first concept for the platform-box, in the inductive conceptual framework, is *Access and Trust*. This encompasses various technological measures in relation to account management and security, such as passwords and other concrete aspects to account security. Furthermore, potential third-party relationships will be discussed, such as BankID and other means of unique identification, while also addressing the ambivalence regarding unique identification and verification of user accounts.

Password Encouragement The biggest "elephant" in the room, that concerns every user of social media platforms, is passwords. NSM (2023a)'s report addresses the concerns regarding weak password practices in Norwegian ICT-systems. Through the interviews, the respondents have not directly stated any concerns regarding weak passwords, rather emphasized that a good password policy and practice is very important, both on an individual- and organizational level.

Although password creation is the user's responsibility, it could be argued that the platforms should provide better solutions to users that does not necessarily prioritize their security online. There is probably little that can be done technically to make people use a unique password for each account, but the platforms could advise their users, for example upon signing up and creating an account, with a pop-up message that informs them that certain tools for generating passwords exists, to help secure the user's accounts by simply informing.

Multi-Factor Authentication On the topic of signing up and creating an account, multi-factor authentication (MFA) is used as an extra layer of security to the login phase to an account, as an extra obstacle for attackers before gaining access to other people's accounts (Kosinski & Forrest, 2024). MFA was a topic that was brought up by several of the respondents. The context to it ranged from emphasizing the importance of it, in addition to encouraging that most people enable this feature, to being more skeptical to force this on everyone.

Most social media platforms do have the option to enable MFA. A concern was raised regarding the average user that might decide against this feature, due to anything from deeming it unpractical to use, to not realizing the risk itself and having the mindset of "No one is interested in me" and "It will never happen to me" - in some cases an act of negligence.

There is little to no doubt that if a user enables MFA, it will increase the level of security to the account. The challenge is to get most people on board with it, and helping them to realize why it is important and why they should enable it. This was also the foundation for the skepticism from R7, as referred to in the last statement in section 4.2.3. R7 discussed that if the social media platforms were to force the use of MFA to every single user, they would risk that a percentage of the users are not able to enable this feature and succeed with it, leading to loss of active users. The reasoning behind this comes down to the economics and the business model that most social media platforms incorporate. With less active users, and therefore less data, the less money generated for the platforms, hence the skepticism to force it from a platform point of view.

If the social media platforms were to force the use of MFA, it could lead to an abundance of inactive and less secure user accounts. These accounts could pose as an attack vector that a social engineer could exploit to manipulate potential victims on social media. In order to mitigate this described risk, the deactivation or removal of these inactive accounts could be considered as a possible solution.

Unique Identification As described in section 2.3.3, the implementation of unique identification could help mitigate social engineering (Osuagwu et al., 2015). Although this has not been tested in any social media platform, to our knowledge, it could still be a viable option, as a user would have to sign up with uniquely identifiable information, rather than having the option to create accounts without any means of authenticity to them.

The topic of unique identification was brought up by R2, stating that this type of unique identification, like BankID, could solve some issues, in regard to fake accounts. On the contrary, this respondent would have been hesitant to sign on with BankID themselves, if it were to be an option. As BankID is merely a Norwegian solution, it would not be applicable to implement to social media platforms, but a more universal solution for the world's population. It would be implausible that every country in the world would be able to have their own unique identification solution, hence the need for a global solution. The ambivalence regarding unique identification could be grounded in that some people do not want to share too much personal information online, essentially being quite anonymous, and using social media platforms as a way to communicate effectively with certain people.

If we were to envision that Meta were to implement a global solution as a way of authentication and verification, this would retrieve personal and sensitive information about the user, and also display this as part of the profile information on the social media platform. The average user might not care, as long as it works, but others may be more restrictive in what information they are comfortable with sharing. This way of authentication, with a plenti-

ful supply of personal and sensitive information at its core, could potentially result in an increase in attempts of data breaches to the platforms, to retrieve this valuable information.

Verified Accounts Apart from unique identification itself, a similar topic was discussed concerning platform verification. On social media platforms, such as Instagram and LinkedIn, there are features that enable users to verify their accounts and get a verification badge on their profile, as a symbol of verification to other users. More often than not, we primarily see celebrities and other individuals with a higher social role having this verification badge, as they usually have a fee to them, at least on Instagram. On LinkedIn, users are able to verify their accounts through their organization or university, along with a similar visible verification badge on their profile.

In regard to social engineering, the discussion of the impact verified accounts could have on both how social engineers would conduct themselves to the matter, and whether it may would have an impact on the awareness of users, was raised. As this is merely a "nice to have"-feature, and not a feature that every user have to enable and make use of, the number of fake accounts would perhaps not be reduced, but it could impact the cautiousness of users.

5.2.2 Defense

The second concept is *Defense*, which will address the use of Artificial Intelligence, in attempt to analyze certain groups and topics on social media platforms and predict events before they happen, to hopefully prevent, or at least being aware of them, and being more proactive.

Artificial Intelligence (AI) Prior to conducting the interviews, we thought that the topic of AI was going to be a major talking point throughout the interviews - however, this was not the case. Although some respondents touched upon the topic, the answers were rather vague and not providing any specific countermeasures. The general perception of the use of AI among the respondents is that it is not advanced enough today. The respondents that discussed AI, also believed that it may well be a solution at some point in the future.

As described in section 2.3.1, Homsi et al. (2021) and Thuraisingham (2020) explain that AI could be used to detect fake accounts, malware, and fake news, among other. In relation to social media, a user is at risk to face all three of them through social engineering. Perhaps the most predominant risk being fake accounts, where there are few possible technological measures to prevent this on social media platforms today.

In addition to this, the Yue et al. (2019) emphasize the use of sentiment analysis (p. 617–618). Through the interviews, some respondents described the process of sentiment analysis without explicitly labeling it as sentiment analysis. This was brought up in regard to the respondents discussing that AI, in general, would not necessarily result in direct prevention of social engineering, rather as a measure of prediction.

The relation between the general perception of the respondents and the proposed measures in the literature is contradictory, but the respondents do not explicitly deny that AI could be used as a countermeasure to social engineering. A plausible explanation to this could be that the use of AI is not that visible to the average user of social media. With AI mostly running in the background, the user might not be aware that it is affecting them, hence influencing their opinion on the use of AI in social media.

5.2.3 Security Governance

The last concept, from a platform point of view, is *Security Compliance*. More specifically, this concept highlights the opinions and reflections regarding the responsibility the social media platforms have when it comes to handling reports in a proper and serious way.

Reporting Mechanisms In relation to the topic of the existing reporting mechanisms on social media, some respondents expressed a concern about the fact that there usually have to be a high number of reports on the same content or profile for it to be taken care of. Most relevant for this research is the profile aspect. It may be difficult for the platforms to deal with reported profiles with only one or two reports to it, as they may seem either legit to the naked eye or have no suspiciousness to them. Vilk and Lo (2023) investigates the concept of reporting mechanisms in social media platforms, where they address how the lack of efficient reporting mechanisms are an issue, in addition to the underlying reasons as to why they claim that such mechanisms are "deeply flawed".

Vilk and Lo (2023) further discuss that if the communication between the platform and the users were considerably enhanced, in addition to more user-friendly and accessible, it could improve the efficiency of the reporting process, along with the user experience, essentially making the user feel like they are seen and heard. Through the interviews, some respondents addressed the aspect of whether the platforms would directly benefit from this, and they also expressed an uncertainty regarding whether more advanced reporting features would be beneficial for them. Several respondents argued that one important aspect that the social media platforms look at when considering adding functionality is whether they are able to profit off of it.

5.3 Individual

The second section of the discussion encompasses the human aspect and users of social media, and what responsibilities these individuals have when it comes to protecting themselves against social engineering attacks. Opposed to the previous section, *Platform*, that encompassed the technical measures that the social media platforms are responsible for being implemented, this section will be more user-focused and highlight important aspects that individuals have to consider when using a social media platform.

5.3.1 Awareness

The first concept within the individual aspect is *Awareness*. With a reported 74 % of all cyber incidents including some form of human element (Hylender et al., 2023, p. 8), the human factor in cyberattacks is a problem. Instead of targeting systems with potentially multiple layers of security on several levels, threat actors tend to focus more on individuals that are more easily fooled and manipulated (He, W. and Zhang, Z. J., 2019, p. 249). Ikhalia et al. (2019) emphasizes the need for security awareness measures tailored to the users of social media platforms in order to mitigate social engineering attacks (p. 1277).

Responsibility Awareness When conducting interviews, there were various angles of approach when the respondents discussed the responsibility individuals have to their own security on social media platforms. Some respondents discussed that a level of awareness regarding what a particular social media platform could do with the data and information that a user is sharing, is important to know. This type of information is typically found in the terms of use, but the reality is that a very small percentage of people actually engage and read this information. It was further discussed that a different form of sharing this information could help to preach the message, such as videos or other content that are more

easily digested than text.

Regardless of whether an alternative form of displaying and conveying the terms of use from the platform's side were to be added or not, it is still the responsibility of the individuals to actually familiarize themselves with this information. Marwick et al. (2017) share a similar view regarding the responsibility, essentially stating that the individual users are responsible for all of their action on social media (p. 1–2). R8 discussed a logical mindset that they believed most individuals should apply before making the decision of signing up and making an account (see section 4.3.1). The three-step thought process being: *"Do I really need this?", "What are the conditions?", "What kind of security does this platform provide me, and how do I use it?"*. With this thought process or a similar one being applied before signing up, it is up to each individual to assess whether they are willing to take the risk.

The three-step thought process encompasses merely a logical mindset, rather than emphasizing the technical aspects. This could imply that there is not necessarily a need for delving into the technicalities as an individual on social media to best understand the risks of using them. If users apply common sense and the attempt to understand the basics of the terms of use, hence being more aware and sceptical in general, it could reduce the risks and likelihood of falling victim to a social engineering attack.

Loss of Control An interesting statement was brought up by R7, regarding sharing content on social media platforms, in addition to coloring personal profiles with an array of information to make it look complete. When a piece of information is shared, either personal or other general information, a user have essentially lost control. The responsible user is no longer in control of who has been able to get a hold of this information, and it could potentially be misused.

Hajli and Lin (2016)'s main focus point in their paper is the perceived control of users of social media, which could be considered the same concept as loss of control, in some regard (p. 111–113). Perceived control in social media refers to that users are of the perception that they are in control of their information and assets, when the reality is that once the information is shared, the control is lost. When control is lost, it poses a risk of privacy invasion and exploitation from a social engineer (Hajli & Lin, 2016, p. 113).

It was further elaborated by R7 that the average user might not be aware of the fact that you are not in control of that piece of information now that it is shared online. Even if the responsible user is to delete it, they would never know how many people have seen it and if there are any people with malicious intent that have spotted it that could misuse it.

The message of this statement is basically that all information you share as a user on social media, or online in general, have the potential to be used for other purposes, and that people should therefore think twice before they share that piece of information, essentially losing control.

Abstract Interactions Regarding the loss of control, an analogy was presented concerning physical- and digital interactions by R8 (see section 4.3.5). It was put into the context of driving a car, where one hopefully realize the consequence of driving without brakes, but with digital interactions they might be more abstract and difficult to see the direct consequence of. Furthermore, there might not be a direct consequence either, as it could potentially take years between a user posting or sharing content or some other piece of information and it being misused.

In general, it may be more challenging to realize the danger and consequences before it is experienced, both with reckless car driving and being victim of cybercrime. The digital, more abstract, interactions are just as important to realize the consequences of, as they could result in physical danger in the utmost consequence, either as in physical pain and hurt, or as in the loss of a job or something else of value in life.

5.3.2 Competency

The second concept regarding the individual aspect of social media is *Competency*. The *Awareness* and *Competency* categories are closely related, where it requires a certain competency to be aware, but also the need of awareness to realize that competency in the field is important. A topic that was brought to our attention through several interviews, was the reflections regarding both awareness and some form of education from an early age.

Educating Children Several respondents brought up the topic of how social media and digital tools and services have taken a big role in our lives, including the upbringing of children. With consuming content through TikTok and YouTube, children are being exposed to the entire spectrum of both good and bad. At an early age, children are generally more susceptible to what comes our way, without a sense of criticism.

As we do not have any literature that support nor deny any statements to this topic, but something we found interesting as the interviews went on, supplementary questions were asked, especially regarding how this could be included as a part of the school curriculum. One response, that stood out, in particular, was to make it a classroom discussion, rather than something that should be included in textbooks and concrete learning material. Furthermore, it was stated that children usually tend to come up with the right or reasonable answers to bigger questions and discussions, so instead of having the teachers preach about the topic with what is good and bad, make the children reflect and discuss the issue.

Even though the first statement, regarding content consumption through TikTok and YouTube, may build more into the domain of mis- and disinformation, there is still a need for a certain emphasis in school to prepare the children on the real world. If children were to become more aware and making this a talking point, both as a classroom discussion and a casual conversation, it would be a good start.

5.3.3 Behavior

The last of the three concepts to the individual aspect is *Behavior*. This encompasses certain security behavior that users of social media exhibit, more specifically regarding password creation and the overall perception of how users of social media behave in regard to security.

Password Hygiene Although there is coverage on the password aspect in the literature, this does not address the password behavior and regime people tend to have when creating or updating their passwords. This was a topic that was discussed in the interviews by several respondents, where the emphasis on not re-using passwords across multiple accounts, and the use of long and strong passwords were encouraged. R2 brought up the attack method of handshake hacking or capturing, and recommending the use of long passwords rather than strong passwords, as this method uploads the captured password to a server with immense computational power to display it in plain text. Even though this method mainly applies to Wi-Fi-passwords, rather than passwords on social media, the message is still viable as the use of long passwords that has a personal meaning to the individual, might be preferred.

Furthermore, on the topic of password behavior, it was mentioned that it is perceived that most users tend to find an easy way out when confronted with a set of password requirements, basically implying that the requirement of symbols, a minimum number of letters and so on, is working against it intended purpose.

Comparing the first statement regarding handshake hacking, and the second statement about how people tend to find the easy way out of password requirements, it could be argued that these two statements have the same message, implying that long passwords could be preferred ahead of strong passwords, only with different rationals.

Password Managers Regardless of whether passwords are long or strong, or maybe even a good mix between the two, the use of password managers were a hot topic and discussed by a number of respondents. The reasoning behind it is both aligned with the essence of the previous section of long and strong passwords, but also that the password manager generates a unique password for each account you sign up to, in addition to having the passwords being stored in a secure manner.

Reflecting on the use of password managers, they could be a helpful tool to increase the account security by generating long and strong passwords, essentially lifting much of the password-burden off the users. It is understandable that the average user may have some difficulties with having a unique password for each account online and remembering that account-password link from memory, hence stating the practicality of password managers.

5.4 Organization

The third and last section of the discussion focuses on what organizations can do to educate their employees on safe use of social media. It became clear during the interviews that organizations play a big role in educating their employees on cybersecurity, in general, but also when it comes to safe use of social media. Several of the respondents stated the importance of their employees in securing organizations, with specifically pointing out how better security regimes for their employees can directly benefit and make organizations more secure. Furthermore, several of the respondents suggested both strategical- and operational measures that organizations could use to educate their employees in safe use of social media.

5.4.1 Defense

This part of the framework, *Defense*, encompasses the different measures that an organization could utilize in an attempt to raise their employees' awareness- and competency levels, hence strengthening their cyber resilience.

Training and Awareness One of the main talking points during the interviews was the need for training- and awareness programs, even though there was a broad consensus between the respondents that these types of programs was necessary, many of them had different ideas for how these could be implemented.

As described in section 2.4.1, a common issue with training and security awareness programs, in organizations, is that often employees feel that they are not relevant nor interesting, often feeling that they are way to generic (He, W. and Zhang, Z. J., 2019, p. 250). This was also brought up by our respondents during the interviews, many of them touched upon and mentioned ways which could encourage their employees, further helping them raising the awareness levels. The training and awareness concept could be considered an umbrella term

for other measures in regard to awareness- and competency enhancement, such as onboarding, risk and consequence, gamification, and repetition.

Onboarding One of the areas that the respondents brought up as an arena for educating and training employees, in both cybersecurity and safe use of social media was onboarding. Onboarding meetings and activities are one of the first things you as a new employee attend after starting a new job. When new employees are presented with information during the onboarding phase, this information could be an indicator for the employees to get a feel for the organization's values and philosophy. Furthermore, it is perceived that employees are usually more susceptible to information during this time, as they want to make a good impression to their new employer.

The general perception of onboarding, in general, is that the structure and content could be considered as generic, and borderline a burden to complete. This is especially relevant where online courses and material are the requirement, where the employees prioritize to complete it at a fast pace, rather than actually learning something from it. To remedy this challenge, the nine core ideas from He, W. and Zhang, Z. J. (2019) could be applied, such as making the information sharing and the overall onboarding experience *fun*, *interactive*, *relevant*, and *rewarding* (p. 252–253).

Risk and Consequences In section 2.4.1, He, W. and Zhang, Z. J. (2019) describe nine core ideas, which organizations can utilize for their security awareness and training programs, with the first one of these being *Accountability* (p. 252–253). This was also brought up by several of the respondents, then in the context of risk and consequence. Some of them argue that focusing on and educating employees on what risks users of social media platforms expose themselves too, as well as what consequences they might face, should they become a victim to a social engineering attack, through social media. Making employees aware of the risks and consequences might have a positive effect on their behavior and awareness, leading to a smaller chance of them falling victim of such attacks. Most people might not know what being present on social media entails, especially from a cybersecurity view, and making then understand the risks and consequences, could absolutely have a positive effect.

One of the biggest issues with educating an organization's employees on the risks and consequences of using social media is the fine line between enhancing their knowledge, and scaring them. It was mentioned by several of the respondents that this line can be hard to balance, and that finding that right balance is important for it being successful.

Gamification Introducing gamification as a tool for education has been suggested already in the literature. McHatton and Ghazinour (2023) suggest a tool called Digital-PASS, which is a gamification tool specifically for social media, and to learn users what risks are associated with using these platforms (p. 30). During the interviews, R10 brought up the concept of learning cybersecurity as a game. R10 explained that people are more willing to learn through games, because the user gets a score, and there might also be a leaderboard for users to compete on.

In this day and age, more and more people are engaging with games or other sorts of digital entertainment. Trying to introduce gamification into education of cybersecurity might be a good platform to use, also for organizations. This also correlates well with most of the nine core idea for successful training programs, as described in section 2.4.1. Gamification can be both fun, interactive, bring some sort of reward, as well as giving the users a feeling of being hands-on with the learning experience. Such platforms will also open up the possibilities of updates, making sure that the content stay relevant and up to date.

Repetition The last point of the defense section is repetition. There was a lack of information in the literature regarding repetition, and this was brought to our attention during the interviews. Several of the respondents discussed the need for repetition, when educating employees. R4 and R10, in particular, discussed the need for repetition. They both explained how people often forget what they have been taught, that people in general will forget more and more over a period of time, until they eventually start to take shortcuts instead of doing what they have been taught. Organizations need to understand that educating their employees on cybersecurity and social media, can not be treated a one time tactical thing, rather it must be a strategic ongoing effort from the organization.

5.4.2 Behavior

In this framework, *Behavior* refers to employees compliance with an organizations rules and policies. The behavior of an organization's employees can play a big role in the organizations cyber resilience.

Rules and Policies Along with the need for training programs, several of the respondents mentioned the need for rules and policies for social media usage. As earlier described in section 2.3.2, organizations often utilize policies and rules for other aspects, such as passwords and the use of multi-factor authentication. Several of the respondents pointed out the importance of having rules and policies in place, it does not only tell the employees what is expected of them and what they are allowed to do and not, but it also gives organizations the opportunity to enforce these rules and policies, should there be some wrongdoing.

What these rules and policies should include will vary from organization to organization. R5 mentioned the possibilities of having separate rules and policies for using social media, as an addition to already existing rules and policies in the organization. These guidelines should apply to all employees in an organization, not just them who uses social media on the behalf of the organization.

Official rules and policies, in combination with educating employees on the possible risks and consequences of using social media, can be an effective way of raising the minimum knowledge level of employees, which can have a positive impact on the employee and the organizations cyber resilience.

5.4.3 Operations

The last concept of the organization section is *Operations*, and it encompasses the organizational culture and the top management support. This concept lacks literature, and the concept of management support and strategies was brought to our attention by the respondents throughout the interview process.

Management and Top-Level Support The respondents discussed the importance of having the management onboard when changing the culture of an organization, and especially R7, in particular, stated that if you want to change the culture, you have to start with the management. Shaikh and Siponen (2023) also address the importance of the top management's attention to cybersecurity and stress the need for investing adequately before a data breach could occur (p. 6–7). R5 elaborates that this will vary from organization to organization, but that for most organizations they need to start with raising the awareness of the management, to further strengthen the employee's awareness.

It is more likely that if there is a foundation of cybersecurity culture starting from the top management, that this will have a positive influence on the employees, and raising their

awareness- and competency levels. In order to achieve a top management focus on investment in cybersecurity, the language of business, more specifically the financial aspect, could be effective to illustrate the urging need (Shaikh & Siponen, 2023, p. 6–7).

Strategy and Clear Philosophy Along with educating the management, as well as the employees, several of the respondents mentioned the need for a clear philosophy and strategy about cybersecurity and social media. The respondents discussed how big the role of social media in organizations has become, and with that comes a need for clear strategies for using these platforms. R5, in particular, mentioned the need for such strategies - they mentioned that these strategies must include information about how these platforms are being used, and what it entails for both the users and the organization. They also extend this to all outreach activates an organization has, along with understanding how to use it, they also need to know how to control it, and most importantly, know what to do if something would go wrong when using these platforms.

Similar to the concept of *Management and Top-Level Support*, a strategic approach to the topic of cybersecurity, essentially investing and being proactive as a means to try and prevent the occurrence of social engineering attacks and to mitigate the risks, if an attack should occur. This would call for a clear philosophy and preaching these principles to the employees and other staff members, in order to pervade the entire organization.

5.5 Implications

Social engineering and social media are two separate and renowned topics that have been well researched respectively, but research that combines the two are rather limited. The research area and problem, which have been investigated during this thesis, is important and heavily relevant, and there is a possibility that this study can be useful for both coming research and professional practice. We believe that this master thesis covers an important research area of the combination between social engineering and social media, encompassing a wide lens that covers the social media platform's responsibilities and possibilities, the individual's responsibilities and the required knowledge and awareness for mitigating the risks of being victim to a social engineering attack, and what organizations could do to educate and tutor their employees in safe use of social media. Furthermore, we encourage that more researcher delve into this topic and investigate the matter further, both through other topics within the domain and through some of our suggestions and findings in this thesis.

From a practical standpoint, the findings of this thesis might be useful, both on an individual- and organizational level. For individuals, this thesis highlights some things that users of social media can do themselves, to bolster their own cyber resilience, and to help protect themselves from social engineering attacks on social media platforms. For organizations, this thesis also suggests some measures that organizations can utilize to better help their employees ensuring their safety on social media, which will also indirectly raise the cyber resilience of the organization itself.

5.6 Limitations of This Thesis

In a master thesis, as with all other research projects and studies, there are limitations that needs to be addressed. First of all the time frame of the thesis, along with the limited amount of resources available during the study, made it so we had to make some compromises.

Secondly, the sample size used during the empirical data collection of this thesis, can be seen as a limitation. The sample size restricted us from seeing the results from a broader view, something we would have been able to do with a larger sample size. Together with the sample size, the diversity of the respondents could also be seen as a limitation of this thesis. With a larger sample size, we would have been able to put together a even broader and more diverse group of respondents, making it possible to investigate the research problem from even more angles.

With the adaptation of the Cybersecurity Culture Framework (figure 2.1) as a basis for structuring this research project, this could be considered as both a positive, in terms of adapting an already existing framework, but also a negative, in terms of the potential for a narrow-minded and too specific approach to the research area. When structuring and planning the interview phase, we based the majority of the interview questions on the selection of concepts. There is a potential that the scope of the questions is too explicit to the concepts, hence the potential for exclusion of other relevant concepts.

5.7 Future Research

The opportunities for future research on the topic of this master thesis are plentiful. There are limited amounts of literature and research available about the use of social media in social engineering attacks, or in cybersecurity as a whole, which make all new research in this field valuable. The first suggestion for further research would be to expand upon this master thesis, it would be beneficial to expand the amount of respondents, and to include a even more diverse set of respondents. Broadening both the amount of respondents and the diversity among them, would hopefully give more valuable insight into this interesting and important topic.

Secondly, each of the three research questions in this thesis can be broken down into separate research topics. This thesis covers three considerably large research areas, and it would be interesting and maybe beneficial to specifically look closer into each of the research areas on its own. By investigating one area at a time, researchers would be able to better understand the respective areas, giving them better insight, which could lead to even more interesting findings in each area. An example of how to more specifically research the platform aspect would be to apply other methods of data collection in addition to the existing interviews, such as extracting data on what measures are already in place on the social media platforms.

As a final suggestion, we recommend to research the root cause of this master thesis, being using social media to conduct social engineering attacks. This could be done by looking into how social engineering is conducted on social media, looking at what techniques are being used, what is most effective, and also how it differs from other types of social engineering attacks. Most people are using social media, so to understand how these platforms are used to manipulate these users, could be highly beneficial.

Chapter 6

Conclusion

The objective of this master thesis is to look into the use of social media to conduct social engineering, and especially to look into which countermeasures can be utilized to mitigated these types of attacks. We identified three research questions, which cover both the technical countermeasures, from a platform point of view, as well as looking into what individuals themselves can do, and lastly looking at what organization can do to educate their employees on safe use of social media.

To answer the three research questions, we have combined the findings from both the systematic literature review and the semi-structured interviews with the ten respondents, in section 5.

RQ1: *Which technologies and measures exist to help secure users of social media platforms from social engineering attacks?*

The findings and discussion for RQ1 are presented in section 4.2 and 5.2, respectively. Based on the inductive conceptual framework (section 5.1), the first research question is categorized as *Platform*. The main focus for this research question is the technical aspects to the topic of social engineering and social media, addressing mostly the social media platform's responsibilities and opportunities for securing their users to a better extent.

There are three main takeaways from this first research question. The first one being the use of BankID or a similar unique identification method for authentication purposes. The use of a unique identification method would make the identification of every user of social media have personal identifiable information to it, hence the opportunity to trace any wrongdoings back to an individual. Even though it could be considered as controversial, it is still a viable option. Secondly, the general perception of the use of AI in mitigating social engineering on social media, is that the AI is not advanced enough at this moment in time. Even though the technology for detection of fake accounts and bots are available, the scale of which these threats occur is considered by the respondents as not advanced enough. Lastly, there is an emphasis on good and effective reporting mechanisms. The users must be able to report their cases in a effective, but detailed manner, leading to higher efficiency and accuracy for the social media platforms to take action.

RQ2: *What responsibilities lie on the users of social media platforms to protect themselves against social engineering attacks?*

The analysis of RQ2 is presented in 4.3 and 5.3, which call for the *Individual*-aspect in the inductive conceptual framework. The emphasis for this research question is more focused on what the users of social media platforms themselves are responsible for, in regard to what

they can do to mitigate being victim of social engineering attacks.

Through the analysis of this research question, we have identified three main takeaways, similar to the previous research question. Firstly, both already existing users and potential users of social media platforms have to be aware of what they are signing up for. In many regards, this is already available for the users to familiarize themselves with through the terms of use, but the reality is that next to none is actually reading this. As a platform's responsibility, it is suggested that this information was to be made available in some other content form than a long text-based report, as it may would help the users to consume the information in a different way. Nevertheless, the emphasis on knowing the terms of use is important before signing up.

The second takeaway addresses that most users of social media platforms do not realize that once a piece of content or information is shared, this piece of content or information is out of their control. Even if the user would be able to delete it, the spread of the data is unknown and could be at risk for misuse. Lastly, the education of children about the topic of social media and overall risks associated with being online became central through several interviews. To not necessarily preach about the topic and scaring the children, but rather making it a classroom discussion topic and talking about it, would in most cases result in the children coming up with rational answers themselves. With the high digital dependence in all aspects of life today, the content and use of social media and digital tools could have a high impact on people's behavior, hence the importance of emphasizing critical thinking and good cyber hygiene from an early age.

RQ3: *How can organizations educate their employees in safe use of social media to reduce the occurrence of social engineering attacks?*

The findings and discussion of RQ3 are presented in section 4.4 and 5.4, respectively. This research question is based on the *Organizational*-section of the inductive conceptual framework, where the focus is on what organizations can do to educate their employees on safe use of social media.

We have throughout the analysis of this research question found several interesting methods, that organizations could utilize. First of all, there was a high focus on having training programs and education for employees, particularly focusing on the onboarding phase. Most companies have some sort of onboarding program when new employees are enrolled into the organization, and utilizing this phase to introduce new and important concepts, can be beneficial. When new employees are being enrolled into an organization, they are often more susceptible to new information, as they usually aim to make a good impression. All the information and presentations that are being presented during the onboarding process, could often make the new employees getting a feel for what the organization believe is most important.

Secondly, for the content being delivered during training and awareness programs, we noticed that many of the respondents mentioned the importance of learning their employees about the risks and consequences that a possible cyberattack would have. Even though focusing on the risks and consequences could be beneficial for organizations, there is a fine line between making them more aware and scaring them. Along with educating employees on the risks and consequences, we also found that repetition is key to educating your employees. People tend to forget what they have been taught, and after a period of time without training, they will get back to old and bad habits, taking shortcuts instead of doing what they have been taught. Organizations need to take this into account, making sure that core and important

aspects are being repeated to their employees, on a regular basis.

The final two key findings of this research question are the focus on having rules and policies in place, as well as having the backing of the management and having clear strategies and philosophies for cybersecurity and safe use of social media. Having rules and policies in place, makes sure that the employees of the organizations know what is being expected of them, as well as telling them what is allowed or not. It also gives the organization a chance to enforce, should there be any wrongdoing from the employees. For the management support, it was noted that to change your employees behavior, an organization needs to start by changing the behavior of the management. Lastly, it was noted that the work on cybersecurity and safe use of social media is not a one time tactical thing, rather it needs to be a strategic and ongoing focus of an organization.

Bibliography

Abu-Nimeh, S., Chen, T., & Alzubi, O. (2011). Malicious and Spam Posts in Online Social Networks. *Computer*, *44*(9), 23–28. https://doi.org/10.1109/MC.2011.222

Aichner, T., Grünfelder, M., Maurer, O., & Jegeni, D. (2021). Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019. *Cyberpsychology, Behavior, and Social Networking*, *24*(4), 215–222. https://doi.org/10.1089/cyber.2020.0134

Algarni, A., & Xu, Y. (2013). Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models. *International Journal of e-Education, e-Business, e-Management and e-Learning*, *3*(6), 456–462. https://doi.org/10.7763/IJEEEE.2013.V3.278

Aun, Y., Gan, M.-L., Wahab, N. H. B. A., & Guan, G. H. (2023). Social Engineering Attack Classifications on Social Media Using Deep Learning. *Computers, Materials & Continua*, *74*(3), 4917–4931. https://doi.org/10.32604/cmc.2023.032373

BankID. (n.d.). *Hva er egentlig BankID?* https://bankid.no/hva-er-bankid Retrieved 28. May 2024.

Bishop, M. (2019). Healthcare Social Media for Consumer Informatics. In M. Edmunds, C. Hass, & E. Holve (Eds.), *Consumer Informatics and Digital Health: Solutions for Health and Health Care* (pp. 61–86). Springer International Publishing. https://doi.org/10.1007/978-3-319-96906-0_4

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.2007.00393.x

Breda, F., Barbosa, H., & Morais, T. (2017). SOCIAL ENGINEERING AND CYBER SECURITY. *INTED2017 Proceedings*, 4204–4211. https://doi.org/10.21125/inted.2017.1008

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

Caramancion, K. M. (2020). An Exploration of Disinformation as a Cybersecurity Threat. *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, 440–444. https://doi.org/10.1109/ICICT50521.2020.00076

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

Gamallo, P., & Almatarneh, S. (2019). Naive-Bayesian Classification for Bot Detection in Twitter. *Conference and Labs of the Evaluation Forum*. https://api.semanticscholar.org/CorpusID:198489886

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, *62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare*, *10*(2), 1–19. https://doi.org/10.3390/healthcare10020327

Gomes, V., Reis, J., & Alturas, B. (2020). Social Engineering and the Dangers of Phishing. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–7. https://doi.org/10.23919/CISTI49556.2020.9140445

Grant, C., & Osanloo, A. (2015). Understanding, selecting, and integrating a theoretical framework in dissertation research: Developing a 'blueprint' for your "house". *Administrative Issues Journal Education Practice and Research*, *4*(2), 12–26. https://www.researchgate.

net/publication/266015734_Understanding_selecting_and_integrating_a_theoretical_framework_in_dissertation_research_Developing_a_'blueprint'_for_your_house

Grønmo, S. (2016). *Samfunnsvitenskapelige metoder* (2. ed). Oslo: Fagbokforlaget.

Hai Wang, A. (2010). Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach. In S. Foresti & S. Jajodia (Eds.), *Data and Applications Security and Privacy XXIV* (pp. 335–342). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-13739-6_25

Hajli, N., & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, *133*, 111–123. https://doi.org/10.1007/s10551-014-2346-x

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102–113. https://doi.org/10.1016/j.cose.2017.10.008

He, W. and Zhang, Z. J. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

Homsi, A., Al-Nemri, J., Naimat, N., Kareem, H. A., Al-Fayoumi, M., & Abu Snober, M. (2021). Detecting Twitter Fake Accounts using Machine Learning and Data Reduction Techniques. *Proceedings of the 10th International Conference on Data Science, Technology and Applications - DATA*, 88–95. https://doi.org/10.5220/0010604300880095

Hylender, D., Langlois, P., Pinto, A., & Widup, S. (2023). *2023 Data Breach Investigation Report* (tech. rep.). Verizon. https://www.verizon.com/business/resources/Tf16/reports/2023-data-breach-investigations-report-dbir.pdf

IBM. (n.d.). *What is natural language processing (NLP)?* https://www.ibm.com/topics/natural-language-processing Retrieved 12. February 2024.

Ikhalia, E., Serrano, A., Bell, D., & Louvieris, P. (2019). Online social network security awareness: mass interpersonal persuasion using a Facebook app. *Information Technology & People*, *32*(5), 1276–1300. https://doi.org/10.1108/ITP-06-2018-0278

Jeong, B., Yoon, J., & Lee, J.-M. (2019). Social media mining for product planning: A product opportunity mining approach based on topic modeling and sentiment analysis. *International Journal of Information Management*, *48*, 280–290. https://doi.org/10.1016/j.ijinfomgt.2017.09.009

Kavin, B. P., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., Haleem, S. L. A., Jose, D., Tirth, V., Kshirsagar, P. R., & Adigo, A. G. (2022). Machine Learning-Based Secure Data Acquisition for Fake Accounts Detection in Future Mobile Communication Networks. *Wireless Communications & Mobile Computing*, *2022*, 1–10. https://doi.org/10.1155/2022/6356152

Kosinski, M., & Forrest, A. (2024, January 4). *What is MFA?* https://www.ibm.com/topics/multi-factor-authentication

Leyrer-Jackson, J. M., & Wilson, A. K. (2018). The associations between social-media use and academic performance among undergraduate students in biology. *Journal of biological education*, *52*(2), 221–230. https://doi.org/10.1080/00219266.2017.1307246

Lindemulder, G., & Forrest, A. (2024, April 8). *What is open-source intelligence (OSINT)?* IBM. https://www.ibm.com/topics/osint

Marwick, A., Fontaine, C., & Boyd, D. (2017). "Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. *Social Media + Society*, *3*(2), 1–14. https://doi.org/10.1177/2056305117710455

McHatton, J., & Ghazinour, K. (2023). Mitigating Social Media Privacy Concerns - A Comprehensive Study. *Proceedings of the 9th ACM International Workshop on Security and Privacy Analytics*, 27–32. https://doi.org/10.1145/3579987.3586565

Mughaid, A., Al-Zu'bi, S., Al Arjan, A., Al-Amrat, R., Alajmi, R., Abu Zitar, R., & Abualigah, L. (2022). An intelligent cybersecurity system for detecting fake news in social media websites. *Soft Computing: A Fusion of Foundations, Methodologies and Applications*, *26*, 5577–5591. https://doi.org/10.1007/s00500-022-07080-1

Narayanan, V., Robertson, B. W., Hickerson, A., Srivastava, B., & Smith, B. W. (2021). Securing social media for seniors from information attacks: Modeling, detecting, intervening, and communicating risks. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 297–302. https://doi.org/10.1109/TPSISA52974.2021.00053

NSM. (2023a, February 13). *Risiko 2023* (tech. rep.). https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2023

NSM. (2023b, November 15). *Ti sårbarheter i norske IKT-systemer* (tech. rep.). https://nsm.no/regelverk-og-hjelp/rapporter/ti-sarbarheter-i-norske-ikt-systemer

O'Connor, C., & Joffe, H. (2020). Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines. *International Journal of Qualitative Methods*, *19*. https://doi.org/10.1177/1609406919899220

Osuagwu, E. U., Chukwudebe, G. A., Salihu, T., & Chukwudebe, V. N. (2015). Mitigating social engineering for improved cybersecurity. *2015 International Conference on Cyberspace (CYBER-Abuja)*, 91–100. https://doi.org/10.1109/CYBER-Abuja.2015.7360515

PAN. (n.d.). *Pan is a series of scientific events and shared tasks on digital text forensics and stylometry*. https://pan.webis.de/ Retrieved 28. May 2024.

Rebeca. (2023, November 27). *Social engineering, an invisible threat: Trends and developments*. Altospam. https://www.altospam.com/en/news/social-engineering-an-invisible-threat-trends-and-developments/

Recker, J. (2021). *Scientific Research in Information Systems: A Beginner's Guide*. Springer. https://doi.org/10.1007/978-3-030-85436-2

Rengamani, H., Kumaraguru, P., Chakraborty, R., & Rao, H. R. (2010). The Unique Identification Number Project: Challenges and Recommendations. In A. Kumar & D. Zhang (Eds.), *Ethics and Policy of Biometrics* (pp. 146–153, Vol. 6005). https://doi.org/10.1007/978-3-642-12595-9_19

Rodriguez, A., & Okamura, K. (2019). Generating Real Time Cyber Situational Awareness Information Through Social Media Data Mining. *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, *2*, 502–507. https://doi.org/10.1109/COMPSAC.2019.10256

Rowe, F. (2014). What literature review is not: diversity, boundaries and recommendations. *European Journal of Information Systems*, *23*(3), 241–255. https://doi.org/10.1057/ejis.2014.7

Rudra, A. (2023, March 9). *Social Media Social Engineering: Understanding the Risks on Online Platforms*. PowerDMARC. https://powerdmarc.com/social-media-social-engineering/

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 1–8. https://doi.org/https://doi.org/10.1016/j.cose.2022.102974

Sliva, A., Shu, K., & Liu, H. (2019). Using Social Media to Understand Cyber Attack Behavior. In J. I. Kantola, S. Nazir, & T. Barath (Eds.), *Advances in human factors, business management and society* (pp. 636–645, Vol. 783). https://doi.org/10.1007/978-3-319-94709-9_62

Templier, M., & Pare, G. (2015). A Framework for Guiding and Evaluating Literature Reviews. *Communications of the Association for Information Systems*, *37*, 112–137. https://doi.org/10.17705/1CAIS.03706

Thuraisingham, B. (2020). The Role of Artificial Intelligence and Cyber Security for Social Media. *2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, 1116–1118. https://doi.org/10.1109/IPDPSW50202.2020.00184

University of Houston - Clear Lake. (n.d.). *Password Attacks and Countermeasures*. https://www.uhcl.edu/information-security/tips-best-practices/pwattacks Retrieved 28. May 2024.

Vilk, V., & Lo, K. (2023, June 29). *Shouting into the Void: Why Reporting Abuse to Social Media Platforms Is So Hard and How to Fix It* (tech. rep.). PEN America. https://pen.org/report/shouting-into-the-void/

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, *8*, 85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), 13–23. http://www.jstor.org/stable/4132319

Wilson, D. W., Lin, X., Longstreet, P., & Sarker, S. (2011). Web 2.0: A Definition, Literature Review, and Directions for Future Research. *AMCIS 2011 Proceedings - All Submissions*, 1–10. https://aisel.aisnet.org/amcis2011_submissions/368/

Wolf, M., Sims, J., & Yang, H. (2018). Social Media? What Social Media. *UK Academy for Informations Systems Conference Proceedings 2018*, 1–18. https://aisel.aisnet.org/ukais2018/3/

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, *39*(1), 93–112. https://doi.org/10.1177/0739456X17723971

Yue, L., Chen, W., Li, X., Zuo, W., & Yin, M. (2019). A survey of sentiment analysis in social media. *Knowledge and Information Systems*, *60*, 617–663. https://doi.org/10.1007/s10115-018-1236-4

Appendices

A Interview Guide

Interview guide

We appreciate that you want to participate to our master thesis interview. The purpose of this interview is to investigate how social media is used in social engineering attacks, how the users of social media platforms can be secured from a technical and non-technical point of view, in addition to how organizations could best educate their users in safe use of social media. We have conducted a literature study prior to the interviews, where we have collected and analyzed related information regarding the topic. The insight and data collected through the interviews will be compared with the findings from the literature study to give us the best possible understanding of our research questions.

The interview is anonymous, and all data collected will be anonymized prior to inclusion in the final report. The interview will be video- and/or audio recorded for us to transcribe. By the end of the project all recordings and documentation, that includes personal information, will be deleted. The end date for the project is estimated to 07.06.2024. You are free to not answer some or all our questions, without the obligation to provide any reason as to why you do not wish to answer. The information and data that will be collected through the interview process will be analyzed and used in the master thesis, «How to protect users on social media platforms from social engineering attacks».

If you are willing to participate and signing the consent form, you consent to that the students by the University of Agder, Daniel Bergmann and Christian Solheim, on the master's programme Cybersecurity Management, can use the data collected through the interview in their master thesis. This data will only be processed by Daniel Bergmann and Christian Solheim, before it will be anonymized.

The interview will have a semi-structured format, where it will be asked questions in relation to social media and social engineering attacks, in addition to the opportunity for us to give some follow-up questions where we see this fit. The questions can be seen below.

The estimated timeframe for the interview is 30-40 minutes.

Part 1: General information

1. What is your education level and programme?
2. What position and work experience do you have?
3. Do you trust that social media, such as Facebook, X and LinkedIn ensures your safety online?
4. How do you see the risk of using such platforms?
    a) Is there a difference between work and private use?

Part 2: Social engineering in social media

1. What are your thoughts on the use of social media in social engineering attacks?

2. How is it used? What kind of techniques are used to attack a user through social media?

    a) Which techniques do you consider as most effective?

3. How would you describe the responsibility of a user of social media when it comes to securing their own accounts?

4. How can this be mitigated?

    a) What should the users do?

    b) What countermeasures exist on a technical level?

5. What do you think an organization should do to increase the level of awareness and knowledge for their employees on the use of social media?

    a) What do you think is the most effective measure(s)?

6. Is there something else you would like to add to the subject?

Part 3: Feedback

1. Do you have any feedback on the structure or process of the interview?

B Consent Form

You want to attend the research project *How to protect users on social media platforms from social engineering attacks*

The purpose of the project

This is a question to you if you want to attend this master thesis project where the purpose is to investigate which technologies and measures exist to secure users of social media platforms from a technological perspective, as well as what the users should do to protect themselves. Based on the purpose of this study we have created these research questions:

1. Which technologies and measures exist to help secure users of social media platforms from social engineering attacks?
2. What responsibilities lie on the users of social media platforms to protect themselves against social engineering attacks?
3. How can organizations educate their employees in safe use of social media?

Information collected as a part of this master thesis will only be used for its intended purpose.

Why are you being asked to attend this project?

The selection of interviewees is personnel with a technological aspect in their job position. This is because the purpose of the research has a two-sided angle; a technological and a human aspect. Through this purpose, we ensure that it is most appropriate and useful to gain insight from professionals who work within the technological aspects of IT and cyber.

Who is responsible for this research project?

The research team consist of two master students, Daniel Bergmann and Christian Solheim, from the University of Agder at the faculty of social science and department of information systems, who are responsible for processing the personal data in this research project.

Participation is voluntary

It is voluntary to participate in this research project. If you choose to participate, you can withdraw your consent until the 10th of May 2024. The reason for defining a date for the withdrawal of your consent is so we can remove all information from the project, both about you and the valuable insight you have given to the project, before our delivery deadline, 7th of June 2024. It will not have any negative consequences for you if you decide not to participate or if you withdraw your consent.

What does participating mean for you?

We will collect information and insight during the interview. It is possible for both digital and physical interview. In the case of a physical interview, an audio recording will be made of the interview. In the case of a digital interview, video recording will be used.

Information which will be collected about you:

- Name
- Education
- Job title
- Work experience

If you want to contribute to the master thesis and decide to attend the interview, we estimate the duration of the interview to be between 30 and 40 minutes. The content and questions which will be asked during the interview concern your thoughts and experiences about cybersecurity in social media, as well as the risks of being targeted by a social engineering attack. Examples of questions during the interview:

- General information about you
    - Education
    - Job title and work experience
- What do you think about the use of social media in cyberattacks?
- What do you think about a user of social media platforms, responsibility to secure themselves?
- How can we mitigate such attacks?
    - What should the users do?
    - What sort of technical countermeasures exist?

Privacy – How do we store and process your information

We will only use your information for the purposes explained in this document. We process all personal data confidentially and in accordance with the privacy regulations.

- Only data controllers, Daniel Bergmann and Christian Solheim, will have access to your information.
- Only data controllers, Daniel Bergmann and Christian Solheim, will collect, process and store your information.
- Measures in place to make sure that unauthorized persons don't get access to your personal information:
    - Your name will not be a part of the interview, only for invitation and other forms of contact, and it will be anonymized
    - Company name will be anonymized
    - The collect data will be stored in Microsoft Teams, where only the data controllers will have access, with multifactor authentication enabled

In the final report attendees will not be recognizable. Alle attendees will be fully anonymized and will be referred to as numbered interview objects, maybe with job title where this is appropriate. Anonymization measures in place:

- Information which can lead to identifying you will either be deleted, rewritten, or categorized
- Video- and audio recordings will be deleted after the transcription has been completed

What happens to your personal information when the research project is concluded?

The research project will, as it stands now, be concluded on the 7th of June 2024. All information will be fully anonymized for potential further analysis until the 31st of December 2024. After this deadline all information will be deleted from all media.

What gives us the right to process personal information about you?

We process your personal information based on your consent.

On behalf of the University of Agder, the privacy services at Sikt - the Knowledge Sector's service provider have assessed that the processing of personal data in this project is in accordance with the privacy regulations.

Your rights

If you can be identified in the data material, you have the right to:

- to request access to the information we process about you, and to be given a copy of the information,
- to have information about you corrected that is incorrect or misleading,
- to have personal data about you deleted,
- to send a complaint to the Norwegian Data Protection Authority about the processing of your personal data.

We will give you a reason if we believe that you cannot be identified, or that your rights cannot be exercised.

Questions

If you have any questions or wish to exercise your rights, please contact:

- Christian Solheim, christiaso@uia.no
- Daniel Bergmann, danielber@uia.no
- Jaziar Radianti, jaziar.radianti@uia.no, (Supervisor)

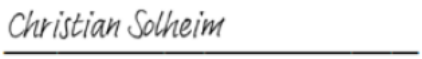
- Our privacy commissioner: Trond Hauso, personvernombud@uia.no, +47 936 01 625

If you have questions related to Sikt's assessment of the project, you can contact us by e-mail: personverntjenester@sikt.no or by telephone: +47 73 98 40 40.

Best regards

Christian Solheim

(Student)



Daniel Bergmann

(Student)

Jaziar Radianti

(Supervisor)

I have received and understood the information about the project "How to protect users on social media platforms from social engineering attacks" and have had the opportunity to ask questions. I agree to:

- Participating in the interview
- That Christian Solheim and Daniel Bergmann can give information about me to the project

I consent to my information being processed until the project is finished

_____

Project participant, date

C Overview of SLR articles

Author	Title	Year
Abu-Nimeh, S., Chen, T. & Alzubi, O.	Malicious and spam posts in online social networks	2011
Aichner, T., Grünfelder, M., Maurer, O., & Jegeni, D.	Twenty-five years of social media: A review of social media applications and definitions from 1994 to 2019	2021
Algarni, A., & Xu, Y.	Social engineering in social networking sites: Phase-based and source-based models	2013
Aun, Y., Gan, M.-L., Wahab, N. H. B. A., & Guan, G. H.	Social engineering attack classifications on social media using deep learning	2023
Bishop, M.	Healthcare social media for consumer informatics	2019
Boyd, D. M., & Ellison, N. B.	Social network sites: Definition, history, and scholarship	2007
Breda, F., Barbosa, H., & Morais, T.	Social engineering and cyber security	2017
Caramancion, K. M.	An exploration of disinformation as a cybersecurity threat	2020
Carley, K. M.	Social cybersecurity: An emerging science	2020
Gamallo, P., & Almatarneh, S.	Naive-bayesian classification for bot detection in twitter	2019
Gomes, V., Reis, J., & Alturas, B.	Social engineering and the dangers of phishing	2020
Hai Wang, A.	Detecting spam bots in online social networking sites: A machine learning approach	2010
Hatfield, J. M.	Social engineering in cybersecurity: The evolution of a concept	2018
He, W., & Zhang, Z.	Enterprise cybersecurity training and awareness programs: Recommendations for success	2019
Homsi, A., Al-Nemri, J., Naimat, N., Kareem, H., Al-Fayoumi, M., & Abu Snober, M.	Detecting twitter fake accounts using machine learning and data reduction techniques	2021
Ikhalia, E., Serrano, A., Bell, D., & Louvieris, P.	Online social network security awareness: Mass interpersonal persuasion using a facebook app	2019
Jeong, B., Yoon, J., & Lee, J.-M.	Social media mining for product planning: A product opportunity mining approach based on topic modeling and sentiment analysis	2019
Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D.	A cyber-security culture framework for assessing organization readiness	2022
Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C.	A cybersecurity culture survey targeting healthcare critical infrastructures	2022

Kavin, B. P., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., Haleem, S. L. A., Jose, D., Tirth, V., Kshirsagar, P. R., & Adigo, A. G.	Machine learningbased secure data acquisition for fake accounts detection in future mobile communication networks	2022
Leyrer-Jackson, J., & Wilson, A.	The associations between social-media use and academic performance among undergraduate students in biology	2018
McHatton, J., & Ghazinour, K.	Mitigating social media privacy concerns - a comprehensive study	2023
Mughaid, A., Al-Zu'bi, S., Al Arjan, A., Al-Amrat, R., Alajmi, R., Abu Zitar, R., & Abualigah, L.	An intelligent cybersecurity system for detecting fake news in social media websites	2022
Narayanan, V., Robertson, B. W., Hickerson, A., Srivastava, B., & Smith, B. W.	Securing social media for seniors from information attacks: Modeling, detecting, intervening, and communicating risks	2021
Osuagwu, E. U., Chukwudebe, G. A., Salihu, T., & Chukwudebe, V. N.	Mitigating social engineering for improved cybersecurity	2015
Rengamani, H., Kumaraguru, P., Chakraborty, R., & Rao, H. R.	The unique identification number project: Challenges and recommendations	2010
Rodriguez, A., & Okamura, K.	Generating real time cyber situational awareness information through social media data mining	2019
Sliva, A., Shu, K., & Liu, H.	Using social media to understand cyber attack behavior	2019
Thuraisingham, B.	The role of artificial intelligence and cyber security for social media	2020
Wang, Z., Sun, L., & Zhu, H.	Defining social engineering in cybersecurity	2020
Wilson, D., Lin, X., Longstreet, P., & Sarker, S.	Web 2.0: A definition, literature review, and directions for future research	2011
Wolf, M., Sims, J., & Yang, H.	Social media? what social media	2018
Yue, L., Chen, W., Li, X., Zuo, W., & Yin, M.	A survey of sentiment analysis in social media	2019