Fool Me Once, Shame on Me - A Qualitative Interview Study of Social Engineering Victims

Silje Berg[1,2 [0009−0004−7908−0986]], Tilde Thorvik[1,3 [0009−0000−8738−9466]], and Per Håkon Meland[1,4 [0000−0002−5509−0184]]

[1] NTNU, Trondheim, Norway
silber@alumni.ntnu.no, tildegt@alumni.ntnu.no, per.hakon.meland@ntnu.no
[2] Mnemonic, Oslo, Norway silje@mnemonic.no
[3] Netlight, Oslo, Norway tith@netlight.com
[4] SINTEF Digital, Trondheim, Norway per.h.meland@sintef.no

Abstract. Security breaches still continue to flourish despite of the many technical measures in place. More often than not, the human users get the blame. Social engineering attacks use various manipulation techniques to fool users into giving away sensitive information or make security mistakes that are further exploited in cyber attacks. This study has investigated how common, cyber-enabled social engineering attacks, such Business Email Compromise (BEC) phishing and romance scams can be used to exploit individuals, systems or organizations. We investigate studies from the literature and apply a qualitative approach based on in-depth interviews with sample victims of such attacks. Our results contribute to the understanding of why established social engineering protection measures sometimes fail and how the victims have experienced the aftermath of such events. Based on our findings and literature comparison, we provide reflections on how mitigations can be improved to reduce the success rate of social engineering attacks.

Keywords: social engineering · shame · victimization · romance scam · phishing · interview

1 Introduction

Social engineering was originally coined by economist John Gray already in 1842 [17] and can be understood as the art of using manipulation and psychological persuasion to make people compromise information systems [25]. More than 150 years after Gray, Schneier [41] stated that "only amateurs attack machines, professionals target people". Security breaches continue to flourish, and humans are frequently referred to as the weakest link and the ones to blame, both in academic papers as well as the media [1, 3, 16, 18, 23, 26, 32]. This could be because social engineering attacks are commonly used as gateways for other more sophisticated attacks [53]. According to Verizon's Data Breach Investigation Report for 2022, 82% of all security breaches include human actions [49]. However, there are also advocates for the humans, claiming that this blame is rarely justified

[53, 56, 10]. We should rather rethink how we build our systems, working procedures, trust, company cultures, responsibilities and supporting mechanisms. Humans are difficult to upgrade and patch, and blaming them does not seem to help tackling the attacks.

To address these challenges, there is a need for more interdisciplinary research to better understand why social engineering attacks are so successful. According to Washo [50], social engineering research lacks a framework to view the topic and to apply findings in real-world organizational settings. *Security economics*, as proposed by Anderson [6], allows researchers to describe information security shortcomings from an economic perspective, leading to a better understanding of why security breaches still occur despite robust technical measures. In addition to economic concepts, such as *information asymmetry*, *misaligned incentives* and *externalities*, security economics has come to include concepts from *behavioral economics* and *psychology* as well. Since social engineering relies on using psychological tricks on the victim, it seems fruitful to look into how these concepts can be used as a framework for the following research questions:

- *Why do theoretical solutions to social engineering issues not always work out as expected in reality?*
- *Which measures can reduce the success rate of social engineering attacks?*

Our study combines theory from the literature with reflections from a sample of victims of real-life incidents to answer these questions. We focus on the prevalent social engineering attack types *Business Email Compromise (BEC)* phishing and *romance scams*, but believe the results are transferable to most of the other variants as well.

Section 2 gives an overview of the central social engineering attack types for our study, and briefly introduces the related work on which we are leaning on. Section 3 explains our methods, before our results are presented in Section 4. These results are discussed and reflected upon in Section 5, and Section 6 concludes the paper.

2 Background and related work

There are forms of social engineering attacks that have existed as long as mankind itself, and new ones appearing alongside with new technological developments. Ivaturi and Janczewski [21] created a taxonomy to give an overview of the different types, separating between direct person-person interaction and interaction via some other medium, such as cyberspace. Koyun and Al Janabi [24] have done similarly with their social engineering taxonomy, splitting between human-based and computer-based types. They argue that the latter makes use of technology to interact with a large number of victims at once. Literature surveys by Salahdine and Kaabouch [40] and Aldawood and Skinner [5] show more than twenty categories, which again can be divided into sub-categories. For instance, *phishing attacks* can be divided into *spear phishing*, *whaling phishing*,

vishing phishing, *interactive voice response phishing*, and *business email compromise phishing*. In our study we have focused on two prominent types of social engineering attacks, namely *business email compromise phishing* and *romance scams*. According to Verizon [48], *phishing* is the most common and widespread form of social engineering. Here, the attacker primarily uses email in order to reach a large number of potential victims, both organizations and individuals. Attackers depend on persuasion techniques that make the attacker seem trustworthy, likable and have a sense of authority [14, 22]. *Business Email Compromise* (BEC) is a type of phishing attack [2], which relies on email fraud that targets organizations by making it seem as if the sender of the email is legit and a trusted party. Within the BEC category, there are *CEO fraud*, *invoice fraud*, *blackmailing emails* and others as well.

Romance scams is believed to be a common and among the most lucrative cyber-enabled scams for criminals according to Yen and Jakobsson [54]. It belongs to the *advance fee fraud* category, where the objective is to steal large sums of money from targeted victims [51]. The criminals typically create false profiles on online dating sites or social media, and establish a false relationship with their victims. Thus, they are targeting both the heart and purse of their victims through digital means.

In the literature there are many examples of related social engineering studies. Longtchi et al. [30] have recently performed a literature study on why social engineering attacks succeed despite of so many proposed defense techniques. They have found that defenders tend to prefer technical solutions, but that does not match well with attacks based on psychological techniques. Based on the original work of Mitnick and Simon [33], many (e.g., [5, 34, 40]) describe a common pattern or cycle of steps for social engineering attacks, consisting of *i)* researching/information gathering about the victim(s), *ii)* building trust with the victim, *iii)* exploitation of trust, and finally *iv)* execution/exit. In contrast to these studies, we have taken the viewpoint of the victim, hence it is stages *ii-iv*, along with the aftermath of the attack, where we relate our findings.

Most existing social engineering victimization studies are in the form of questionnaires. For instance, Whitty [51] has investigated the personal characteristics of romance scam victims in the UK through an online questionnaire. Studies from Renaud et al. [38] and Budimir et al. [9] investigate the emotional responses of victims after security incidents. Workman [52] has conducted another social engineering field study covering 588 respondents using a questionnaire. The Norwegian Business and Industry Security Council conducts a bi-annual phone survey related to security incidents within private and public organisations. The 2022 edition [35] included 2500 respondents, and when asked about why security breaches could occur, the main given reason was "coincidence or bad luck" (61%). The next prominent reasons were "human error" and "lack of security awareness".

More similar to our interview study, is for instance Banire et al. [8]. They collected data from 20 victims and found that the outcomes of successful social engineering are mainly due to five factors; absent-mindedness, ignorance of

attacks, inadequate security measures, situation (circumstance) of the victim, and trusting stolen identities of personal contacts. In an interview study of 16 undergraduate students in the UK [11], concepts such as gullibility, weakness and naivety were all mentioned in the context of cybercrime victimization.

There are also examples of studies investigating the offending side of such attacks. For instance, Steinmetz et al. [44] have interviewed 37 professional and nonprofessional social engineers to find out which traits can be associated to vulnerable organizations.

3 Methods

Qualitative research, such as interviews, focus on gathering insights of the experiences of people [12]. Though it might not be possible to generalize the findings to entire populations, the results might challenge or confirm established truths, discover local variations and provide new insights that should be investigated further. Compared to existing social engineering victimization studies, which tend to collect quantitative data through surveys, we have in our study chosen to go more in-depth with a smaller group of respondents to collect details on their personal perspectives.

We chose semi-structured interview as the main data collection method. An interview guide ensured that the interview touched upon the specific topics we were interested in. This is not as strict as a structured interview, allowing for follow-up questions where this is deemed valuable [47]. Before collecting our interview data, we applied to and got an approval from the *Norwegian Agency for Shared Services in Education and Research* that the treatment of personal information was in accordance with the *Personal Data Act*. This act incorporates the *European Data Protection Regulation* (GDPR). The interview guide consisted of reflection questions about the incident, such as how the victims experienced it, attitude on security, why the attack succeeded, how it was perceived by others and what could have been done differently. A transcript of the interview guide can be found in the Appendix.

Finding victims of social engineering attacks willing to come forth is a known challenge. In our case, a sample of respondents were recruited through convenience sampling, meaning contacting people who had already talked publicly about their incident or people in our professional network we knew had been attacked. All respondents were interviewed during the Spring of 2022. The interviews were performed through video calls due to spread localization and restrictions from the COVID-19 pandemic. They lasted up to 90 minutes and were recorded, with the consent of the interviewees, transcribed and coded. Coding qualitative data turns the raw data into a story by identifying the most relevant topics and elements by labeling words, paragraphs, and sentences with a word or a phrase that summarizes the content [29]. Our codes were based on central concepts from the literature on social engineering and extended inductively based on new themes that were identified during the transcription phase.

Table 1. Characteristics of the incidents

Attack	Type and exposure	Victim
A	BEC, publicly known	University hospital
B	BEC, anonymous	Private service company
C	Romance scam, publicly known	Private person
D	BEC (artificial), anonymous	Private IT company

4 Results

The next section describes the attacks based on the victim stories. The following sections correspond to the coding system that we used during the analysis of the interviews transcriptions. We have included what we consider to be the most relevant findings.

4.1 Attacks and victims

Our study encompasses four social engineering attacks with their own distinct characteristics. Table 1 shows an overview of the attacks and victims, which are further detailed below based on the explanations of the victims.

Attack A: In 2019 the University of Tromsø (UiT) planned to buy a new medical computerized tomography (CT) scanner from a British supplier. The supplier sent the invoice over email, which is standard procedure for foreign suppliers. The following day the same person at UiT received an email that seemingly was from the supplier, asking when they could expect the payment. The email domain was not from the supplier, but the UiT employee did not notice this, thus the BEC attack was in motion. The email contained a lot of information from the original invoice that UiT received the day before, and the UiT employee regarded it as a genuine inquiry and answered in the same email thread. The imposter asked if UiT could change a bank account number, and gave a credible explanation to why this was necessary, which included practical challenges regarding Brexit. UiT made the payment of €1.2 million to the new bank account number and discovered some weeks later that the money was lost. UiT went public with this story to increase internal and external awareness of such frauds, and one representative (Victim A) volunteered to be an informant in our interviews.

Attack B: This incident is similar to A, but seen from the other side of a corrupted payment transaction. Victim B represents an anonymous service provider company, where the attacker intersected the communication between the company and one of their clients in a man-in-the-middle manner. Victim B was supposed to receive payments from their client in two iterations. The first payment appeared as expected, but then the client received an email with a new bank account, and the client transferred the second payment to this one. During this process, both parties received impersonated emails from what seemed to be

the other party. This was discovered after some time, and the client took the burden of a new payment. This incident is still an unresolved police investigation.

Attack C: In 2019, Victim C went public with a story of how a professional social engineer had manipulated her for several months. She met the fraudster through an online dating platform, and started dating him under the impression that he was a wealthy businessman. After some time, they became a couple. Later on, he made her believe that he was in trouble and needed financial help from her. The victim applied for loans in nine different banks in Norway and the United Kingdom and provided him with the money. She eventually realized he was a fraudster and reported him to the police. When she felt like the police did not do enough to solve the case, she told her story to the press, and this story has recurred in various news articles, as well as a documentary on Netflix (*The Tinder Swindler*, released in 2022 also featuring other victims). After the incident, she has acted as a spokesperson for fraud victims claiming that banks, police, and other stakeholders are not helping fraud victims sufficiently.

Attack D: Victim D works in an IT company and received an email that looked like it was coming from his CEO, asking him to click on a link to fill out a survey about the company's state and how the employees were feeling. The company had sent out surveys like this before, and the victim considered the email to be credible. The victim felt encouraged to answer because there were issues he wanted to highlight, but thought it was a bit strange that the deadline was on the same day. The link led him to a Microsoft Single Sign On (SSO) page, where he provided his username and password. Shortly after, he received a message saying he failed security training. This was an artificial attack setup by the company, nevertheless, we found it interesting to investigate how the victim perceived the event and reflected on such exercises.

4.2 Why attacks succeed

Misaligned incentives

> "I feel that the banks can do so much more, but they have zero risk with keeping things the way they are" -Victim C

Misaligned incentives can be an explanation to why social engineering attacks are successful. Misaligned incentives were discussed by almost all interviewees, who had various ideas of how incentives are influencing the success of social engineering attacks.

Victim C brought up that the banks have stronger economic incentives to make it easier to grant consumer loans, than they have ethical incentives to make it harder to get granted a loan in order to protect the customers from scams. She also mentioned that the banks face no economic risk themselves when involved in a scam. She explained that this is because if the bank grant a customer a consumer loan, it falls upon the customer to pay back the loan, even though they were tricked into establishing the loan.

All the victims that reported the incident to the police, Victim A, Victim B and Victim C, described challenges in that process that can be understood

using misaligned incentives. One aspect mentioned by particularly Victim A and Victim C, is that the police are not doing enough for victims of scams. All victims experienced that all or parts of their cases were dropped, despite existing trails of evidence. Furthermore, crimes that involve different police districts, such as Victim B, or go across borders, such as Victim A and Victim C, are described in the interviews as even harder to get the police to look into. Victim A indicated that international complications obstructed further investigation of the incident. Victim A also said that it is hard to discuss the reason of the incident with their supplier because the supplier had incentives not to disclose it due to potential loss of reputation.

4.3 Bad luck

"I don't believe in luck, being lucky or unlucky." -Victim D

Inspired by the findings from the broad survey by the Norwegian Business and Industry Security Council [35], we asked all the interviewees whether or not bad luck could be an explanation to why the social engineering attack was successful.

Most of the interviewees agreed that bad luck was not the main reason behind their incident. They believed that to blame it on bad luck would also make it more challenging to uncover the root cause of the problem. Victim D expressed that if bad luck is a mix of circumstances, having your thoughts in another place and poor training, then maybe. In general, Victim D thought there were a lot of factors playing at the same time. Victim A said that blaming it on bad luck is a way to not take the blame, and that would prevent taking these incidents seriously.

Shame

"It is not embarrassing to be tricked by professionals." -Victim C

Victim C said that one of the reasons she was open in the media about being scammed was to show to other victims of similar scams that it is not embarrassing to be tricked by professionals. She wants to show that victims are not alone in their situation and reduce the shame of falling for social engineering. She thinks a lot of the shame comes from not being seen as a victim by the police and others, and the treatment by others is an extra punishment. Victim C expressed that if the police reinforces the initial shame, victims will not dare to be open about the incident.

Victim A said that UiT had focused on not blaming and shaming individuals for the mistake around the invoice fraud and instead focused on organizational learning and what they need to do differently to avoid similar incidents.

Culture of trust

"Trust is a beautiful and good thing we have in Norway" -Victim C

Several of the interviewees discussed the concept of trust as an important aspect related to social engineering. A recurring explanation from the interviews as to why people generally fall for social engineering attacks is that people want to be helpful to people they trust.

Victim C said that most of her fellow victims easily trust people and want to help out when someone needs them. Even though Victim C trusted the attacker and fell for the scam, she still meant that trust is a good thing and that the trust in Norway is positive. Even though she has suffered substantial economic losses, she still trusts people. She expressed that this is because what happened to her was very special, and her life would be destroyed if she had to be skeptical about every person in her life.

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

Transparency

> "It is important that this incident does not end up in the media" -Victim B

The victims were asked about their opinions regarding transparency related to social engineering attacks and why they chose to or chose not to be transparent about their case. All the interviewees mentioned the importance of being open and transparent about security incidents and that this can reduce successful social engineering attacks due to increased awareness and available information. However, getting people to discuss security incidents is more complicated.

Victim B fears the negative media attention the security incident could cause for his employer and strives to keep it secret and out of the media's attention. Despite withholding his story from the public, he believed that being open about incidents like this would generally be helpful for others. Victim A, on the other hand, chose to be open about the security incident even though they too believed it would negatively impact the reputation of the university. However, Victim A said that there had not been much direct criticism towards the university after sharing details of this incident. He also stated that he has experienced a certain acceptance that it is possible to be deceived, and that the victims do not have all of the blame, even though the incident still negatively affected the reputation. UiT went public with it because of the external and internal benefits of openness. According to Victim A, awareness is the key to preventing attacks like this from happening repeatedly. Furthermore, he expressed that it can reduce the chances of successful attacks when being transparent, especially through sectorial cooperation.

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

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

Humans as the weakest link

> "I think there are other things that are weak links as well, because not every area of what we're doing is up to speed." -Victim D

The claim that humans are the weakest link in a security chain has been widely accepted and established as mentioned in Section 1. The interviewees have different opinions on the matter. Victim A and Victim D expressed that humans are the weakest link if all the recommended security procedures are implemented, but if this is not the case, they do not think humans are the weakest link. Victim B agrees with the claim that humans are the weakest link, and he argues that he thinks humans are too inattentive. In contrast, Victim C disagrees with the statement and argues that automation has more blame than humans.

4.4 Recommended measures

This section presents suggestions given by the interviewees against social engineering attacks. These were identified from questions related to countermeasures. We have mainly included the measures the interviewees meant are important to focus more on.

Security awareness improvements

> "Our people were fooled when they should not have been." -Victim A

Some interviewees expressed that they did not think security training was effective enough and gave recommendations on how this could be improved. For instance, Victim A emphasized that improved awareness, competence and vigilance of social engineering can make the attacks less successful. Furthermore, Victim A believed that focusing not only on countermeasures against social engineering attacks, but also learning about how attackers attempt to attack and scam can be effective.

Victim D wanted to support more technical measures that can help create awareness. For instance, he recommended implementing warnings for emails that come from outside the organization.

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

Better policies

> "The bigger the consequences are for you as a private person, the more manual elements should be included in the process." -Victim C

Victim C said she thought less automation in banks could be useful and could reduce successful attacks or the consequences of attacks. She elaborated that extra verification when doing larger bank transfers than usual could be a valuable policy for the banks to implement.

Victim A suggested that an independent verification channel would help reduce attacks. This recommendation was given in the context of invoice fraud. At the same time, he emphasized that countermeasures cannot be overwhelming and that organizations do not have unlimited resources to spend on measures against social engineering.

5 Discussion and reflection

5.1 Lessons learned

Throughout the interviews, it became clear that there are several explanations for why the theoretically secure solutions that can protect against social engineering attacks fail in practice, giving insight into our first research question. The following sections discuss explanations given by the interviewees, and reflects on how this compares to other studies from the literature. Here, we also highlight which measures that could mitigate social engineering attacks, addressing our second research question.

Aligning incentives According to Norwegian legislation [31], it is the private individuals that are economically liable if they fall for social engineering scams. This is because the banks are only responsible for covering the loss if it is caused by unauthorized transactions, and the transactions in these attacks are normally authorized by the victims themselves. However, according to Anderson [6], this makes the banks careless, which leads to a more significant number of successful scams. Victim C's statements substantiate this. Currently, the banks have stronger incentives for having smooth solutions with high usability to maintain and increase their customer base, than spending extra resources on approving consumer loans. A change in financial liability alignment might motivate the banks to be more supportive to their customers.

Most of the victims talked about challenges with reporting and follow-up from the police. Similar frustrations from victims have been seen in many other cases in Norway, such as [27, 45, 46]. From the police's perspective, this prioritization is understandable given limited resources and competence, and the fact that working across international borders is challenging. However, the consequence of dropping these cases is that the adversaries know that the risk of being caught is low, making the potential payoff worth the risk, thus creating more incentives to do so. Similarly to us, Baddely [7] points to limited capacity of government institutions and small chances of being caught as significant reasons to why attacks prevail. Currently, the Norwegian police does not really know the extend of such cybercrime due to low reporting. Making reporting easier, with better follow-up, would at least give a better picture of the situation, and could lead to additional policing resources and mandates for following up cross-border cases.

Improving transparency Some of the benefits of transparency have been described in previous papers, such as improved probability estimates for decision-makers [42]. One of our main takeaways from the interviews is that transparency should be regarded as an externality when discussing social engineering from a security economic perspective. This is because increased transparency provides increased insights about what we can learn about these attacks, and thus protect ourselves better. Transparency about social engineering incidents should be considered a public good within information security, since the information is non-excluding, being openly available, and non-rivaling, as no single person's use of this information excludes other people's use of the information. At the same time, openness and transparency allows the adversaries to know more about which attacks are successful and could help them adapt their attack patterns. This should be regarded as a negative externality.

We found valuable insight in the cases where the interviewees disagree, most evidently found when comparing Victim B and Victim A's interviews. Both supported transparency as an ideal to improve security. However, unlike Victim A at UiT, Victim B prioritized his employer's need for secrecy. From the interviews we conclude that one negative effect of transparency is loss of reputation, which negatively affects the attacked organization more than the positive externalities from increased transparency. This is an example of how a moral hazard is manifested in the battle against social engineering attacks, because each actor benefits from being selfish and withhold information that can negatively affect their reputation, even though society as a whole benefits from increased transparency. It also shows how transparency as a public good is exposed to the "free rider problem" described by Baddeley [7], where one actor benefits from the transparency of others. Victim A also shared his doubts about everyone being transparent about security breaches. He did not believe their supplier would share information about breaches as they had no incentives to be transparent.

Shame cripples transparency During the interviews, we discovered the importance of shame as an aftereffect of successful social engineering attacks.

Shame can come from the victim's thoughts, for example they can feel that they should have realized what was going on. Shame can also originate from other individuals who blame the victim for falling for the scam. Victim C emphasized that she has encountered several social engineering victims who, like herself, felt shame caused by themselves and how others acted after the attack. The quotes below displays some of the comments people left on social media about Victim C after the incident she was involved in became known.

> "This is exactly what a gold digger deserves, no sympathy from me"
> "Great that she has to pay herself, it's no human right to be in love and stupid. Her greed took the upper hand"
> "Banks can't cover idiocy"
> "It's her own fault, and an expensive lesson learned"

There were also comments and replies in social media defending her actions, as can be seen from the sample quotes below.

> "It is easy to judge other people. Being exposed to a narcissistic, manipulative person is not something to feel ashamed of"
> "Everyone can be fooled, even high-ranked Professors"
> "The criminals go free and the victim is penalized both legally and socially"
> "It is insane that the banks give out consumer loans without any collateral"

Whom to blame is a discussion out of scope for our study, we merely address that public comments like these inflict the feeling of shame both for Victim C herself and others who see them. Though some comfort can be found in supportive comments, social media now function as an enforcer that often feels like an extra punishment for the victim. The study of Renaud et al. [38] also discovered that those who had caused a cyber security incident often felt guilt and shame, and that the responses of their employers either exacerbated or ameliorated these negative emotions. Similarly, the study by Conway and Hadlington [11] found that victim blaming and self-blaming are commonplace. This topic of shame for the victims deserves more extensive studies. From what we gather, it is an important element to consider when looking at why existing countermeasures continue to fail. This is because shame reduces the willingness to be transparent. The victims might also need more time to recover from the attack if they feel stronger shame, which makes the attack even more costly for the affected parties. Budimir et al. [9] conclude in their study that there is a need for emotional support systems that can avoid the negative long-term psychological consequences the victims experience.

Limitations of security awareness training According to Pyzik [37], increased information security awareness is one of the best mitigation measures against a social engineering attack. However, multiple studies [19] conclude that

"traditional security awareness training" that focuses on what employees should and should not do as well as awareness of risks and threats is ineffective in regards to changing employees' behavior.

Another challenge with training is limited efficiency against personalized attacks. Security awareness training can give general advice and raise awareness around attacks and countermeasures, but it is hard to even discover attacks when they are very personalized, as seen with the incidents related to Victims A-D. Malicious use of advanced AI-based techniques, e.g. shown by Lies [28], Guo et al. [15] and Zeng [55], can severely increase the amount and quality of personalized attacks. This is indeed a serious challenge we are facing to an increasing degree. Based on their literature review of social engineering training programs, Aldawood and Skinner [4] suggest to profile at-risk employees and developing more targeted training programs at different levels.

Trust as an asset or a challenge Even though many people participate in security awareness training and hear about security incidents, it is in the human nature to trust people in their everyday life. Trust is, as commonly known, a central tool in almost all social engineering attacks, and can result in that we ignore security training and security policies. Social engineering attackers take advantage of this. From the interviews, we conclude that trust is essential for making people help you and returning favors. A lack of trust will lead to duplicate work through extra checking, decrease productivity and create doubt between co-workers, which can contribute to a negative culture within the organization.

There is a fine line on how much trust we should give people and which precautions to take. The interviews show that too little trust will negatively impact people's lives, but trusting the wrong people or having too much faith that people take sufficient security precautions can lead to severe consequences as seen in Attack A. The colleagues' trust in each other was one of the reasons why the attack succeeded, because everyone assumed that the others had quality-checked the fraudulent email. This is in line with the findings of Banire et al. [8], where misplaced trust in stolen identities of personal contacts is one of the main reasons why attacks succeed.

Strengthening the weakest link Whether humans are the weakest link within security seems to be a subjective perspective, and different opinions also manifested themselves in the interviews. For example, Victim B stated that humans are inattentive and that this is one of the reasons why we are the weakest link. We believe that this mindset has great implications when working to prevent social engineering. This is because the chosen measures to prevent and react to these attacks rely heavily on how you look at humans in the security chain. Looking at humans as the weakest link might lead to a culture where more blame is placed on the person that was tricked even though there are other weaker links in the security chain. We believe this can lead to more shame when being subjected to a social engineering attack, which again can create negative repercussions like fear of telling the IT department. Viewing humans as the weakest link can also

prevent us from finding the root cause as to why the attack was successful and prevent similar attacks, just as blaming bad luck. This perspective can lead to extra awareness training to minimize the damage humans can do, but on the same time, create too demanding policies for so-called misbehavior. The consequence can be security fatigue among users and lack of motivation because it seems hopeless to keep striving for optimal security behavior when you consider yourself as the weakest link no matter what. The paradox Adams and Sasse presented [1] almost 25 years ago, where increased security mechanisms lead to less secure behavior, seems to still be accurate.

According to Whitty [51], there is a popular belief that mostly "stupid" people fall for romance scams. Contrary to this, her study shows that those who were more highly educated were also more vulnerable to becoming romance scam victims. A study by Saad and Abdulla [39] showed that the most likely romance scam victims in Malaysia were well-educated, married and with a good income. Similar findings are reported by Pinto et al. [36] related to phishing attacks. This corresponds to our Victim C, who has a high education and a knowledge-intensive job. Whitty also found that impulsive and trusting people with addictive personalities are likely victims of romance scams. Though we may be able to improve people's awareness, trying to change their personalities is probably not something we should and are able to do.

Security 2 We believe it would be beneficial to switch the mindset from seeing humans as the weakest link to seeing them as a security resource. Such a change of attitude can reduce successful engineering attacks because it can empower and motivate people to pay more attention if they know they can be of assistance.

In line with this empowerment, we want to introduce a new concept, namely *Security 2*, which focuses on the many things that go well instead of only looking at the things that go badly. This is inspired by the *Safety 2* concept from Hollnagel et al. [20], recognizing the capabilities to succeed under varying conditions and emphasizes that more things go well than wrong. People can gain digital confidence by learning about others that have been able to prevent social engineering attack. Based on this, new recommendations on security measures can be developed and shared. Additionally, we believe that this will give people a sense of motivation, making them more inclined to focus on preventing social engineering attacks when they know it is possible.

5.2 Limitations

Local context One commonality among the victims in our study is that they were all in Norway. This local context has a significant since Norwegians in general tend to trust others. They happen to be the most trusting citizens in Europe towards public institutions such as the police or politicians [43]. This was seen as an advantage during the COVID-19 pandemic, when the population trusted the government and promptly followed socializing and vaccination advice. However, overly trust can be a disadvantage for Norwegians in relation

to social engineering attacks. At the same time, Norway is considered to be technologically advanced and an example of a society that depends heavily on information systems, and thus, a society exposed to cyber threats. For instance, Norwegians use digital services well above EU average and companies have a high online presence [13]. We have no real assurance that the cultural combination of trustfulness and being online makes Norwegians more prone to social engineering than other populations.

Different interview coverage The study was based on information gathered from semi-structured interviews, where the focus was to get the interviewees talking, without interrupting them too much. As a result, not all questions were asked to all interviewees, because they either covered the topic before the question was proposed, or the question was deemed less relevant for the current interviewee. Having different questions, and thus answers, made direct comparison between interview results not really possible.

One side of the story The interviewees have only described their own experiences. Particularly with the victims of social engineering attacks, their personal feelings color their experiences and descriptions of what happened, as well as how they felt others perceived what happened. Therefore, a limitation to this study is that we only have presented one side of each attack. We do not know how the other people involved in attack A and B look at the situation. Regarding Victim C's counterpart, we have only registered statements in various media, being very critical towards Victim C. We have chosen not to present such communication in this study. It is therefore likely that our discussion is somewhat biased by the interviewees' perspectives, even though this is something have tried to minimize.

6 Conclusion

We have collected data from victims of social engineering attacks and used concepts from security economics to explain and reflect on our results. To a large extent, our findings substantiate findings from existing literature.

Most of the interviewees shared a common belief on why social engineering attacks are successful. *Misaligned incentives*, *shame*, *culture of trust* and (missing) *transparency* were to a large extent pointed at as the most important factors. Also, defining humans as the weakest link might decrease security because this notion can obfuscate other weaknesses. Therefore, an attitude switch from humans being the weakest link to security resources is necessary. Furthermore, it is important to remove the shame related to being a victim of a social engineering attack. We encourage organizations, as well as the society in general, to respect and support instead of blaming, and focus on how social engineering can be prevented in the future. This can be accomplished by also highlighting successful attack prevention stories to increase awareness and build security confidence.

Acknowledgement

This work has partially received funding from the European Union's Digital Europe programme under Grant Agreement No 101083594 (CyberSecPro). The authors gratefully acknowledge the courage and support from interviewees.

Appendix

Interview guide - Victims

About the attack

1. Can you tell about the attack and what happened?
2. Can you describe the process, the work and what has happened since the attack was discovered place?
3. Do you know who is behind the attack?
4. Why do you think they did this?
5. What costs are associated with the event?

Understanding and prevention

1. Why do you think you and those around you fell victim to such an attack?
2. Why do you think the attack was successful?
3. Why do you think that measures against social engineering attacks do not always work as expected in practice?
4. Before the incident took place, were there procedures that should act as measures against such attacks? Do you now have any measures to prevent such an incident?
   (a) What could you have done to prevent this?
   (b) What could the other actors have done to prevent the attack?
5. Do you think such an attempted attack will happen to you again?
6. Have you received any assistance from the police or similar actors in connection with the attack? Is there something you have particularly appreciated that has been done, or something you have particularly missed
7. Do you feel that there are measures you can take to make sure that something similar does not happen again? Or should such measures be done by someone else? Has any other actor have any incentives to introduce measures to prevent this type of attack?
8. Do you know how to obtain information about possible measures against such attack? Do you think it is easy/difficult to find information about measures that can protect against such attacks?
9. Incentives are largely about the motivation one has for doing an action. A possible reason for insufficient effort on security is misaligned incentives, which means that whoever is in a position to prevent an attack, have no incentives to take restrictive measures. Do you have any thoughts about how misaligned incentives between different actors can affect security within a system or between systems?

10. Externalities take place when an actor exhibits behavior that affects the utility of another actor, without taking into account the cost/benefit to the other party. Examples are network externalities, such as a social medium becoming more useful for each individual member when more join. Negative externalities happen for instance when a factory pollutes the climate, but where the consequence of this is not included in anyone's account, and the consequence of the pollution is ignored. Do you have any examples of how externalities affect security in your organization?

Attitudes

1. Before the incident took place, were attacks like this something you thought about in your everyday work?
2. Why is it important to you that information about this event is not exposed?
3. What do you think about measures such as two-factor authentication? Do you feel it has any value, or is it mostly a frustration to deal with?
4. The Norwegian dark numbers survey shows that the majority of people exposed to a security breach say that the reason was bad luck or coincidence, do you have any thoughts about this?
5. Humans are often seen as the weakest link when it comes to security, what are your thoughts on this?

Follow-up questions

Victim A

1. Is this something you have spoken to the supplier about? Have they been asked to provide such information to you?
2. Do you have stronger routines to deal with this now?
3. Do you feel that your openness around this matter has had any negative or positive effects effects on the reputation of the university?
4. You chose to go public with it, why did you do it, what did you want to achieve with it?
5. Do you have an opinion on which security measures are worthwhile and which are not?

Victim B

1. Do you need to keep things secret as to not expose the others parties?
2. It is a policy where you work that this is not the kind of thing you want publicity on?
3. You are part of an environment with people who work on similar things. Is this something you have talked about with others in the industry?
4. Do you think it would have been useful to talk more about it internally in the industry, given that this could remove the fear of media exposure?

Victim C

1. You talk about several new laws, which ones are you referring to?
2. You mention trust. Trust during the pandemic has been of value, whereas your type of attack targets people who want to trust and be kind. Do you wish you were less trusting? Or would it be a bad thing to be less trustful after your experience?
3. You have gone out publicly and talked about this, why? What do you want to achieve?
4. Do you think shame is the reason why people are not so open about this, or do you think it is something else that makes it embarrassing?
5. You often encounter a conflict between ease of use and security, which also applies here. Can you elaborate on your experiences with this?
6. Do you regret coming forward, or do you feel it was worth it?

Victim D

1. Which best practices do you not follow?
2. Do you think that security training is useful? What do you think can be done to improve the usefulness of it?
3. Are you more security aware now?
4. Do you want your company to implement such security trainings?
5. Were you annoyed by the event? Or were others in the organization annoyed?

References

1. Adams, A., Sasse, M.: Users are not the enemy. Communications of the ACM **42**(12), 40–46 (1999)
2. Alabdan, R.: Phishing attacks survey: Types, vectors, and technical approaches. Future Internet **12**(10) (2020). https://doi.org/10.3390/fi12100168
3. Aldawood, H., Skinner, G.: Educating and raising awareness on cyber security social engineering: A literature review. In: 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). pp. 62–68 (2018). https://doi.org/10.1109/TALE.2018.8615162
4. Aldawood, H., Skinner, G.: Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. Future Internet **11**(3), 73 (2019)
5. Aldawood, H., Skinner, G.: An advanced taxonomy for social engineering attacks. International Journal of Computer Applications **177**(30), 1–11 (2020)
6. Anderson, R.: Why information security is hard - an economic perspective. Seventeenth Annual Computer Security Applications Conference, IEEE pp. 358–365 (Dec 2001). https://doi.org/10.1109/ACSAC.2001.991552
7. Baddeley, M.C.: Information security: Lessons from behavioural economics. In proceedings of Security and Human Behavior 2011 (2011)
8. Banire, B., Al Thani, D., Yang, Y.: Investigating the experience of social engineering victims: Exploratory and user testing study. Electronics **10**(21) (2021). https://doi.org/10.3390/electronics10212709

9. Budimir, S., Fontaine, J.R., Roesch, E.B.: Emotional experiences of cybersecurity breach victims. Cyberpsychology, Behavior, and Social Networking **24**(9), 612–616 (2021)
10. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS quarterly **34**(3), 523–548 (2010)
11. Conway, G., Hadlington, L.: How do undergraduate students construct their view of cybercrime? exploring definitions of cybercrime, perceptions of online risk and victimization. Policing: A Journal of Policy and Practice **15**(1), 119–129 (2021)
12. Denny, E., Weckesser, A.: Qualitative research: what it is and what it is not. England: Wiley Subscription Services, Inc **126**, 369 (2019). https://doi.org/10.1111/1471-0528.15198
13. Digital Single Market: Digital scoreboard (2016), https://ec.europa.eu/digital-single-market/digital-scoreboard, cited 14 Jan 2023
14. Ferreira, A., Coventry, L., Lenzini, G.: Principles of persuasion in social engineering and their use in phishing. In: Human Aspects of Information Security, Privacy, and Trust. pp. 36–47. Springer International Publishing (2015)
15. Guo, S.W., Chen, T.C., Wang, H.J., Leu, F.Y., Fan, Y.C.: Generating personalized phishing emails for social engineering training based on neural language models. In: International Conference on Broadband and Wireless Computing, Communication and Applications. pp. 270–281. Springer (2023)
16. Harbert, T.: The weakest link in cybersecurity (2017), https://www.shrm.org/hr-today/news/all-things-work/pages/the-weakest-link-in-cybersecurity.aspx, cited 14 Jan 2023
17. Hatfield, J.M.: Social engineering in cybersecurity: The evolution of a concept. Computers and security **73**, 102–113 (2018)
18. Heartfield, R., Loukas, G.: A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Comput. Surv. **48**(3) (dec 2015). https://doi.org/10.1145/2835375
19. Hielscher, J., Kluge, A., Menges, U., Sasse, M.A.: Taking out the Trash: Why Security Behavior Change Requires Intentional Forgetting. Association for Computing Machinery p. 108–122 (2021). https://doi.org/10.1145/3498891.3498902
20. Hollnagel, E., Wears, R., Braithwaite, J.: From Safety-I to Safety-II: A White Paper (2015), https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-whte-papr.pdf, cited 14 Jan 2023
21. Ivaturi, K., Janczewski, L.: A taxonomy for social engineering attacks. In: CONF-IRM Proceedings 2011. vol. 15 (2011)
22. Jakobsson, M.: Understanding Social Engineering Based Scams. Springer New York, New York, NY (2016)
23. Klimburg-Witjes, N., Wentland, A.: Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses. Science, Technology, & Human Values **46**(6), 1316–1339 (2021). https://doi.org/10.1177/0162243921992844
24. Koyun, A., Al Janabi, E.: Social engineering attacks. Journal of Multidisciplinary Engineering Science and Technology (JMEST) **4**(6), 7533–7538 (2017)
25. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. : Journal of Information Security and Applications pp. 113–122 (2015)
26. Lebek, B., Uffen, J., Breitner, M.H., Neumann, M., Hohler, B.: Employees' information security awareness and behavior: A literature review. In: 2013 46th

Hawaii International Conference on System Sciences. pp. 2978–2987 (2013). https://doi.org/10.1109/HICSS.2013.192
27. Lepperød, T.: Betalte 3000 kroner for en mobiltelefon han aldri fikk: - Folk er for godtroende [Norwegian] (2 2018), https://www.nettavisen.no/nyheter/innenriks/betalte-3000-kroner-for-en-mobiltelefon-han-aldri-fikk-folk-er-for-godtroende/s/12-95-3423413669, cited 14 Jan 2023
28. Lies, J.: Marketing intelligence and big data: Digital marketing techniques on their way to becoming social engineering techniques in marketing. Int. J. Interact. Multim. Artif. Intell. **5**, 134–144 (2019). https://doi.org/10.9781/ijimai.2019.05.002
29. Linneberg, M.S., Korsgaard, S.: Coding qualitative data: a synthesis guiding the novice. Qualitative Research Journal **19**, 259–270 (2019). https://doi.org/10.1111/1471-0528.15198
30. Longtchi, T., Rodriguez, R.M., Al-Shawaf, L., Atyabi, A., Xu, S.: Sok: Why have defenses against social engineering attacks achieved limited success? arXiv preprint arXiv:2203.08302 (2022), cited 14 Jan 2023
31. Lovdata: Finansavtaleloven, § 35 - Misbruk av konto og betalingsinstrument [Norwegian] (2009), https://lovdata.no/lov/1999-06-25-46, cited 6 June 2022
32. Martens, M., De Wolf, R., De Marez, L.: Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Computers in Human Behavior **92**, 139–150 (2019). https://doi.org/10.1016/j.chb.2018.11.002
33. Mitnick, K.D., Simon, W.L.: The art of deception: Controlling the human element of security. John Wiley & Sons (2003)
34. Mouton, F., Malan, M.M., Leenen, L., Venter, H.S.: Social engineering attack framework. In: 2014 Information Security for South Africa. pp. 1–9. IEEE (2014)
35. NSR: Mørketallsundersøkelsen 2022 [Norwegian] (sept 2022), https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2022-er-na-tilgjengelig, cited 25 Feb 2023
36. Pinto, L., Brito, C., Marinho, V., Pinto, P.: Assessing the relevance of cybersecurity training and policies to prevent and mitigate the impact of phishing attacks. Journal of Internet Services and Information Security **12**(4) (2022)
37. Pyzik, K.: Shutting the door on social engineering. Internal Auditor **72 (5)**, 20–21 (2015)
38. Renaud, K., Searle, R., Dupuis, M.: Shame in cyber security: effective behavior modification tool or counterproductive foil? In: New Security Paradigms Workshop. pp. 70–87 (2021)
39. Saad, M.E., Norul Huda Sheikh Abdullah, S.: Victimization analysis based on routine activitiy theory for cyber-love scam in malaysia. In: 2018 Cyber Resilience Conference (CRC). pp. 1–3 (2018). https://doi.org/10.1109/CR.2018.8626818
40. Salahdine, F., Kaabouch, N.: Social engineering attacks: A survey. Future Internet **11**(4) (2019). https://doi.org/10.3390/fi11040089
41. Schneier, B.: Semantic attacks: The third wave of network attacks (2001), https://www.schneier.com/crypto-gram/archives/2000/1015.html, cited 2 Feb 2023
42. Schulan, A.: Behavioural economics of security. European journal for security research **4**(2), 273–286 (2019)
43. SSB: Nordmenn på tillitstoppen i Europa - SSB [Norwegian]. https://www.ssb.no/kultur-og-fritid/artikler-og-publikasjoner/nordmenn-pa-tillitstoppen-i-europa (2016), cited 25 Feb 2023

44. Steinmetz, K.F., Knight, T., McCarthy, A.L.: Organizational characteristics associated with vulnerability to social engineering deception: A qualitative analysis. Victims & Offenders **17**(3), 421–438 (2022). https://doi.org/10.1080/15564886.2021.1943092
45. Thonhaugen, M.: Tapte over 7 millioner i svindel, politiet henla på dagen: – Drøyt og jævlig [Norwegian] (5 2022), https://www.nrk.no/nordland/tapte-over-7-millioner-i-svindel_-politiet-henla-pa-dagen_-_-droyt-og-jaevlig-1.15972132, cited 22 June 2022
46. Thonhaugen, M., Wilhelms, H.: Kryptosvindelen [Norwegian] (2022), https://www.nrk.no/nordland/xl/kryptosvindel_-mann-ble-lurt-for-200.000-kroner_-men-folk-svindles-for-millioner-1.15846412, cited 22 June 2023
47. Tjora, A.: Kvalitative forskningsmetoder i praksis. 3. utgave. Gyldendal (2017)
48. Verizon: DBIR 2021 Data Breach Investigations Report. Verizon (2021), https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf, cited 14 Jan 2023
49. Verizon: Data Breach Investigation Report (DBIR) (2022), https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf, cited 14 Jan 2023
50. Washo, A.H.: An interdisciplinary view of social engineering: A call to action for research. Computers in Human Behavior Reports **4**, 100126 (2021). https://doi.org/10.1016/j.chbr.2021.100126
51. Whitty, M.T.: Do you love me? psychological characteristics of romance scam victims. Cyberpsychology, behavior, and social networking **21**(2), 105–109 (2018)
52. Workman, M.: Gaining access with social engineering: An empirical study of the threat. Information Systems Security **16**(6), 315–331 (2007). https://doi.org/10.1080/10658980701788165
53. Yasin, A., Fatima, R., Liu, L., Yasin, A., Wang, J.: Contemplating social engineering studies and attack scenarios: A review study. SECURITY AND PRIVACY **2**(4), e73 (2019). https://doi.org/10.1002/spy2.73
54. Yen, T.F., Jakobsson, M.: Case study: Romance scams. In: Understanding Social Engineering Based Scams, pp. 103–113. Springer (2016)
55. Zeng, Y.: Ai empowers security threats and strategies for cyber attacks. Procedia Computer Science **208**, 170–175 (2022). https://doi.org/10.1016/j.procs.2022.10.025, 7th International Conference on Intelligent, Interactive Systems and Applications
56. Zhang, Z.J., He, W., Li, W., Abdous, M.: Cybersecurity awareness training programs: a cost–benefit analysis framework. Industrial management + data systems **121**(3), 613–636 (2021)