Department of Sociology
Master's thesis SOCM04 Cultural Criminology, 30 credits
Spring 2023

Scams and Counter-Scams

An Investigation Into the Deception Tactics of Phone Scammers and Scambaiters

Author: Elina Werther
Supervisor: Sébastien Tutenges

Word count: 21,534

Author: Elina Werther
Title: Scams and Counter-Scams: An Investigation Into the Deception Tactics of Phone Scammers and Scambaiters
Master's thesis SOCM04 Cultural Criminology, 30 credits
Supervisor: Sébastien Tutenges
Department of Sociology, spring 2023

Abstract

The purpose of this thesis is to investigate the techniques that scammers and scambaiters use in phone conversations to deceive each other and accomplish their respective goals. Seeing how the number of people losing money to scams continues to rise every year, there is an urgent need for more research to raise awareness of common scam tactics. It is also highly sociologically relevant to gain an understanding of the phenomenon of deception, and the techniques used. Goffman's theoretical framework and Christie's concept of the ideal victim is utilized to gain an understanding of the performances that scammers and scambaiters partake in, as well as how scambaiters portray themselves as victims. The material used in this thesis consists of ten scambaiting YouTube videos, as well as scam descriptions from online forums. A narrative thematic content analysis is then used to analyze the material. The main findings suggest that the scammers in the videos perform as professional customer support- or technical support workers by using tactics such as flattery, intimidation, and trusting relationships. This puts an expectation on the "victims" to respond appropriately. Moreover, they use impression management to save the show from disruptions and control the manner in which they are portrayed. The scambaiters in the videos commonly play the roles of old, naïve, and un-technological men or women. Although they by Christie's definition cannot be perceived as ideal victims, the roles which the scambaiters play possess multiple of the attributes associated with ideal victimhood. Furthermore, the scambaiters' performances contain a comedy factor, which aims to entertain their audiences while making the scammers lose face.

Key words: scamming, scambaiting, scam calls, victimhood, performances, manipulation, ideal victim(s)

Popular science summary

Scams and other types of fraud have existed for as long as humans have owned assets. In modern times, technological advancements have made a wide range of scams possible, as fraudsters are constantly adapting their methods of reaching potential victims. Most people can probably think of one or more occasion when they have encountered a scam, maybe in the form of an email from an unknown address, a strange pop-up, or a phone call from someone claiming that there is something wrong with their computer. As the number of scams continues to increase, online vigilantes calling themselves "scambaiters" have taken it into their own hands to tackle scammers. They usually do this by pretending to be real victims and speaking to scammers with the purpose of wasting their time, preventing real victims from getting scammed, and entertaining and educating audiences. Although some previous research on the topic has been carried out, there is a general lack of research on scamming and scambaiting. Hence, this thesis aims to understand how scammers manipulate their victims, and how scambaiters in turn manipulate scammers and portray themselves as victims.

Ten videos from scambaiting YouTube channels which contain recordings of conversations between scammers and scambaiters were used to investigate the techniques that both parties use to trick each other during phone conversations. Descriptions of scams on online forums were also used to further understand scammers' deception tactics. The main findings showed that scammers often portray themselves as trustworthy and kind early in their conversations, hoping to gain trust and to establish relationships with their potential victims. They further adapt their manipulation strategies to the individual are speaking with, and according to what they think will result in the most favorable outcome. By the final parts of the conversations, the scammers were often questioned or directly confronted by the scammers, which caused them to try to save their scams while also sometimes using intimidation and threats. The scambaiters in the videos portrayed themselves as people who they assumed to be ideal victims for the scammers, usually as old and un-technologically advanced individuals. By playing along and following the scammers' instructions but also challenging them by questioning the scammers and encouraging comedic interactions, the scambaiters achieved their goals of wasting the scammers' time, while simultaneously entertaining their audiences and ridiculing the scammers.

Acknowledgments

THANK YOU…

…To my supervisor Sébastien Tutenges, who has supported me throughout the writing process and contributed with valuable feedback and advice.

…To both Erik Hannerz and Sébastien Tutenges for these two years at the master's program in Cultural Criminology. You have made it a fantastic experience, and your teachings will stay with me forever.

…To my family and friends, who always believe in me and who have provided me with an immense amount of much-needed emotional support and advice.

Table of contents

Introduction

A news article in the New York Post reports the story of 18-year-old Aurora, who has spent most of her teenage years dreaming about the day she would finally be able to buy her own house. Since getting her first job at 14, she has saved up as much as she possibly can in order to turn her dream into reality. However, in early December 2022 she received a text message that seemed to be coming from her bank, and which stated that someone she did not know was trying to transfer money from her account. Aurora panicked, and quickly dialed the number that was listed at the end of the message. A polite and professional man with a British accent answered her call and instructed her to transfer all her money into a new account in her name, which he was supposedly setting up while speaking to her. The man's professionalism and her own state of panic convinced Aurora to follow his instructions, and she quickly sent him the money. The man then hung up the call. Aurora's entire life savings – over 25 000 Australian dollars – were gone in only a few seconds (Kazlauskas, 2023).

Aurora had fallen victim to a scam, a "deceptive scheme that seeks to trick a person(s) out of money and/or personal information which is unethical and may also be a civil, regulatory or criminal issue too" (Button & Cross, 2017, p. 7). She is far from the only one who has fallen for a scam like this. An article from Comparitech (McCart, 2022) gathered statistics surrounding scam calls, and noted that not only did scam calls increase by 118% from 2020 to 2021, but the number of people who fell victim to these scams also increased with 270% from 2019 to 2020. In 2022, over 68,4 million Americans reported losing money to phone scams, which is the highest number recorded since Truecaller started researching phone scams and spam calls eight years ago (Truecaller, 2022).

In addition to this drastic increase, an undercover investigation done by The Times showed that only about one in 50 reports of fraud ends up with a suspect being caught. (Morgan-Bentley & Good, 2019). In the light of this, cyber-vigilantes who call themselves "scambaiters" have taken it upon themselves to attempt to tackle scammers while simultaneously entertaining audiences. The owners of the YouTube channel "Trilogy Media" – a scambaiting channel – argue that their goal with scambaiting is to help where law enforcement has failed, and to educate viewers about common scams (Deck & Kumar, 2023).

Seeing how the number of people falling victim to phone scams continue to rise every year, it is highly relevant and important to research this area in order to raise awareness about how

the offenders trick people into falling for their scams. Although some previous research has been conducted on scam techniques (e.g., Whitty, 2013; Bakar & Zakaria, 2021; Shaffer; 2012), the majority of these have analyzed victims' stories instead of the scams themselves. Shaffer (2012) did use scam emails as her data, but there are likely differences when it comes to the techniques used in scams conducted via email and scams conducted via phone calls. Research on the phenomenon of scambaiting has also previously been conducted (e.g., Smallridge et al., 2016; Tuovinen & Röning, 2007; Ross & Logi, 2021), but it has mainly focused on scambaiters' objectives, ethical aspects of scambaiting, and scambaiting on streaming sites and social forums. Apart from raising awareness about common scam techniques, research on scams and scambaiting further contributes with sociologically relevant and interesting insights into the world of lies and deception. The purpose of the present thesis is to gain an understanding of the techniques that scammers might use to deceive their potential victims during scam phone calls, as well as how scambaiters portray themselves in their phone conversations with scammers to achieve their goals and trick scammers into believing that they are potential victims. The research questions that this thesis aims to answer are hence:

1. How do scammers verbally manipulate their potential victims through phone conversations?
2. How do scambaiters mislead scammers and perform victimhood through phone conversations?

The thesis will start off by providing background information on the three main subjects of study: scammers, scam victims, and scambaiters. Thereafter, previous research on scamming and scambaiting will be presented, followed by a description of this study's theoretical framework and the methods that are going to be applied to answer the research questions. Then, there will be a discussion on the chosen method and the ethical considerations that were made. Next, the results will be analyzed in relation to the theoretical framework and the previous research. The analysis will consist of two chapters, the first which will aim to answer the first research question and discuss scammers' performances, and the second which will discuss scambaiters' performances and portrayal of victimhood, and hence answer the second research question. Finally, there will be a section on the main conclusions drawn from the analysis.

Scamming and scammers

Although today's definitions of scams and frauds are often linked with modern technology, such as the internet, Button and Cross (2017, p. 6) argue that fraud has occurred for as long as "people have been able to speak and own assets." However, technological advances have made a large number of scams possible, as well as making it easier for scammers to reach a wider range of potential victims. Frauds first started getting perpetrated with the use of technology when the internet was getting more and more relevant in the 1980s (fraud.com, n.d.). An example of these early types of technology-based fraud is scams which tried to trick people into calling expensive phone numbers (ibid.). By the 1990s, online credit card use started becoming more common, but the verification technology was still very new and had plenty of weaknesses. Taking advantage of these weaknesses, scammers managed to get ahold of credit card information (ibid.). Identity theft started becoming prevalent in the later 1990s and early 2000s, when scammers impersonated individuals or took over their online accounts through data breaches (ibid.). With constantly evolving new technology, fraudsters continue to recycle old tactics, as they simultaneously develop new and even more sophisticated scams (ibid.). More recently, the outbreak of Covid-19 was utilized by fraudsters who for example sent out phishing emails and ran fake charities (ibid.). Some of the most common scams used today are technical support scams, banking scams, and dating and romance scams (CISA, n.d.; USA gov, 2022; nt.gov.au, 2015). Technical support scams were previously commonly conducted by scammers based in India who claimed to work for a well-known technological company such as Microsoft, and who in an almost random fashion called individuals to tell them that there was something wrong with their computer (Muncaster, 2023). Today, these scams are often conducted with the use of pop-ups, fake websites, or deceptive ads which appear on computer screens trying to convince individuals that their computer has a virus or that something else is wrong with it (ibid.). The computer's owner will usually also see a phone number that they are instructed to call to get the issue fixed (ibid.). In other words, there has been a shift from scammers calling victims, to victims being lured into calling the scammers.

But who are the scammers? Nigeria has been associated with a number of different scams, such as credit card fraud, forgery, and immigration fraud, which has led to concerns about the country's image (Button & Cross, 2017, p. 28). Many types of cyber-crime, including phishing, have proven to be linked with criminal groups in Eastern Europe, for example

Russia and Romania (ibid.). However, although fraudsters in Nigeria and Eastern Europe are responsible for several scams, it largely differs between different types of fraud (ibid., p. 29). Statistics from the United States Federal Trade Commission showed that the USA are actually responsible for most of the fraud attacks against the USA, while only 6 percent were cross-border frauds (ibid.). Data from ThreatMetrix further showed that the top five countries where scams originate from are the USA, the UK, France, India, and Bangladesh (ibid.).

Although research projects that have used interviews with fraud offenders are very rare, some researchers have attempted to find out why individuals start committing frauds (Button & Cross, 2017, p. 30). For example, Levi (2008a, p. 394) managed to identify three different types of fraudsters:

1. Pre-planned fraudsters: the offenders set up a business scheme in advance with the purpose of defrauding victims.
2. Intermediate fraudsters: the offenders start off with the intention of obeying the law, but later consciously turn to fraud.
3. Slippery slope fraudsters: the offenders generally fall into fraud due to pressure or feelings of having no other choice. For example, the offenders turn to fraud while trying to save a bankrupt business.

Levi (ibid.) further argues that pre-planned fraudsters often pretend to be intermediate or slippery slope fraudsters, since this gives them a chance to minimize the risks of prosecution, conviction, and imprisonment.

Victims of scams

In order to carry out their scams, scammers need to find potential victims. One method of identifying victims is to utilize potential victims lists (Button & Cross, 2017, p. 65). These are customer lists that legitimate businesses use for marketing. Open-source information, such as phone directories or lists of shareholders, can also be used to reach victims (ibid.). Another method that scammers use to find victims are so-called suckers lists, which they purchase from other fraud offenders. These lists contain names and information about individuals who have previously fallen for scams and are therefore seen as likely to be re-victimized (ibid.). Apart from using lists, offenders can utilize social networking sites to identify potential

victims (ibid., p. 66). This method is most commonly used in romance or dating scams, where fraudsters attempt to gain trust from victims by forming relationships (ibid.). In Ponzi schemes, false investment scams, it is common for scammers to target affinity groups with the hope of getting one person hooked and then making that person to spread the word to others, leading to more victims (ibid., 67). Lastly, some offenders use a more straightforward tactic of advertising their fraudulent schemes on websites or in publications (ibid., pp. 67-68).

Although many assume that scams mostly affect the older generation, that is not necessarily true (FTC, 2022). In 2021, people aged 18-59 were 34 percent more likely to lose money to scams than people aged 60 and over (ibid.). However, different age groups are more likely to fall for different types of scams (ibid.). For example, younger people more frequently lose money to online shopping- and investment scams, while older people are much more likely to fall victim to tech support- and lottery scams (ibid.). Additionally, older adults lose significantly larger amounts of money to scams than younger adults and while both age groups get scammed by websites and apps, the older population is typically contacted via phone calls, whereas the younger population tends to get contacted on social media (ibid.).

Despite the fact that anyone can fall victim to scams, there are many stereotypes surrounding scam victims, and they largely tend to be blamed for their victimization (Button & Cross, 2017, p. 117). Although victims cannot be defrauded without their own participation in the scams, many fail to acknowledge that offenders are often extremely skilled when it comes to identifying victims' vulnerabilities and using these to manipulate and exploit them (ibid.). There is a stereotype of victims being gullible, greedy, and uneducated, and therefore to some degree deserving of their victimization (ibid., p. 118).

Apart from financial losses, falling victim to scams can have a number of different devastating impacts on individuals (Button & Cross, 2017, pp. 93). Fraud victims can face as severe consequences as those who have experienced violent crimes, but they do not get the same degree of support or acknowledgment as victims (ibid., p. 94). The most frequently reported impacts experienced by fraud victims, apart from financial loss, are anger, stress, and psychological/emotional suffering (ibid.). Some victims even report problems with family or partner relationships, physical health problems, or severe mental health problems as a result of falling victim to a scam (ibid.).

Scambaiters and the phenomenon of scambaiting

According to Collins dictionary, "scambaiting" is "the practice of pretending to fall for fraudulent online schemes in order to waste the time of the perpetrators" (Collins English Dictionary, n.d.). Smallridge et al. (2016, pp. 60) describe scambaiting as a type of cyber-vigilantism in which scambaiters portray themselves as victims who are unaware of the scam, which they typically do for entertainment reasons and/or to engage themselves with civic duty. While most scambaiters' main goal is to waste scammers' time and prevent them from scamming real victims, others have specific purposes, for example obtaining offenders' bank account numbers or personal information which they can then report to the proper authorities (Whittaker & Button, 2021).

It is common for scambaiters to upload videos of their conversations with scammers to YouTube or other media platforms, where they pretend to fall for the scam while amusing audiences by asking the scammer ridiculous questions and referring to inside jokes with their audience (Deck & Kumar, 2023). Many scambaiting content creators are further based in Europe or North America, and their primary scammer targets are in India (ibid.).

Although most scambaiters on platforms such as YouTube claim that their goals are to educate and entertain the audience while wasting scammers' time, there have been discussions on whether scambaiting is ethical (Schultz, 2022). The scambaiting community has experienced a history of humiliating and sometimes racist practices (ibid.). An example of this can be found in the 419Eater forum, which calls itself "The Largest Scambaiting Community on the Planet" (419Eater, n.d.). It is an online forum created in 2003 with the purpose of tackling the "419 emails" which promise people large amounts of money if they first pay a small fee (Whittaker & Button, 2021). The 419Eater forum tries to incentivize their members by rewarding scambaits with a system of icons (ibid.). Some ways to obtain one of these icons is to present an unusually long scambait, or to get a picture or video of a scammer (ibid.). Although these usually do not cause any harm, some sought-after icons represent actions such as getting a scammer to get a permanent tattoo, or to get them to travel a minimum of 200 miles (ibid.). The forum has also been criticized for racial prejudice, especially towards West African scammers (ibid.).

Previous research

Classical studies have found various techniques that might be used by an individual who is trying to go unnoticed while committing a criminal or deceitful act. In his chapter on "sneaky thrills", Katz (1988) claims that young shoplifters will often use different resources and techniques to construct normal appearances and avoid getting caught in the act. For example, they might consider how "normal" customers typically act while shopping and try to imitate the behavior of this idea of the typical customer (ibid., p. 59). Similarly, Cassiman's (2019) work on "tricksters" – young Ghanian men who create fake profiles on dating sites with the intention of finding people who are likely to provide them with money – shows that these men carefully curate their fake profiles according to their victim' specific taste and desires. Like the young shoplifters, they adopt a new persona to help them achieve their goals.

Although these classical studies highlight important aspects of tricking people and getting away with fraudulent acts, the present paper will focus on contemporary research on scams specifically, in order to gain a better understanding of modern and technology-based scams.

Scams and their techniques

Previous research on different types of scams has shown that scammers utilize a variety of linguistic techniques and narrative strategies to attempt to get money from their potential victims. The articles discussed in this section of the paper have researched scams conducted via email, phone calls, social networking sites, and online dating sites, and have found different techniques that are often used in these types of scams.

Schaffer (2012, pp. 157-179) researched the language utilized in so-called "Nigerian frauds" - emails sent by someone pretending to be a Nigerian official who asks for help moving a large sum of money to another country in exchange for a percentage of said money. The author found that scammers often use words and phrases that point to the urgency of the situation, but also convey kindness and a personal connection. For example, they introduce messages with salutations such as "dear sir/madam" or "dear friend", and end with: "your immediate response will be highly appreciated" (Schaffer, 2012, pp. 165-166). Lester et al. (2020, pp. 163-178) did a study on HMRC and IRS scams - tax scams based on phone calls or emails that appear to be from a reputable source. Similarly to the Nigerian fraud scammers, they try

to develop a trusting, but also authoritative, relationship with their victims to increase the chances of successful scams. The results also showed that in a majority of cases, the scammers were male, had adopted a persona with an English-sounding name, and had an accent that was different from British-English or American-English. They usually asked for victims' personal information and remained patient and calm throughout the conversations.

The authors also found that scammers use different strategies in order to convince and persuade their victims. Schaffer (2012, pp. 167-169) noticed that they use methods such as appealing directly to the recipient, using flattery, and attempting to intrigue them by proclaiming the confidentiality or urgency of their business. While these persuasion strategies seem quite gentle and maybe even "kind", the strategies that Lester et al. (2020, pp. 172-173) identified among tax scammers rather aim to intimidate the potential victims into paying. Most victims were threatened with consequences such as arrests, imprisonment, or social media exposure if they did not comply with the scammers' demands.

But how effective are these techniques when it comes to persuading a potential victim? Bakar and Zakaria (2021) argue that the effectiveness of scammers' techniques depends heavily on the potential victims' personality and susceptibility to persuasion. They found that fear appeals – such as threats – do not actually have a significant impact on people who are highly susceptible to persuasion (ibid., p. 879). The reason for this is that individuals with a high susceptibility to persuasion are prone to taking risks and acting recklessly, and fear suppresses these behaviors. Instead, the authors argue that rational appeals have a stronger impact on these individuals, since they encourage logical reasoning instead of depending on individuals' emotions (ibid.).

Whitty (2013) argues that scamming should not simply be understood as a number of techniques, but as a process that consists of different stages orchestrated to groom the potential victim. She analyzed the online dating scam, which consists of a scammer pretending to initiate a relationship with a potential victim via a social networking site or an online dating site, with the intention to eventually defraud the victim (ibid., p. 2). By conducting interviews with 20 participants who were all victims of scams and carrying out a thematic analysis on the data, Whitty was able to create the *Scammers Persuasive Technique Model*. The model consists of seven stages, which all lead to the victim finally trusting the scammer enough to give them money. According to the model, the process begins with a victim who is motivated to find their ideal partner, and who is then presented with an ideal dating

profile. Then, the grooming process commences. In this stage, scammers try to gain the victims' trust by seemingly providing them with a safe environment in which they can feel comfortable to disclose their secrets, insecurities, and deepest thoughts, while simultaneously using poetic and romantic writing. How well the scammer manages to groom their victim and create an attachment determines whether the victim will end up giving the scammer money or not. At the fourth stage, the scammer starts asking for money. They usually start off with testing the waters by asking for gifts or small amounts of money, and if the victim complies, they continually ask for more money. If the victim has not yet complied and given them money by the fifth stage, the scammer uses a technique in which they ask for a huge favor that most would refuse, and then follow it up with a moderate request instead. In some cases, sexual abuse ensues when the victim reveals that they have no money left to give. The final stage consists of the victim being re-victimized (ibid., pp. 22-30).

Since the Scammers Persuasive Technique Model is heavily geared towards the online dating scam, it is highly probable that it is not completely applicable when it comes to many other types of scams. However, it can still help gain an insight into how different scam techniques can be used in an orchestrated process with the goal of grooming the victim and making them comply. Shaari et al. (2019) analyzed Malaysian online romance scammers' linguistic patterns and conversation styles using Whitty's (2013) model. The researchers concluded that scammers used positive politeness strategies at the early stages of their relationship with their victims, such as claiming common ground, similarities, and indications of interest (Shaari et al., 2019, p. 111). By the end of the relationship, however, the politeness strategy shifts from positive to negative and the scammer becomes more aggressive. The authors argue that this usually happens when the victims realize that they have been scammed and want to end the relationship (ibid.).

Scambaiting

Researchers on the subject of scambaiting have previously analyzed the main objectives of scambaiting, as well as how these are achieved through the usage of digital platforms. Although far less research has been conducted on scambaiters and the phenomenon of scambaiting than scams in general, this section will discuss the works of four groups of researchers who have explored how scambaiters utilize digital platforms in order to achieve

their goals and reach large audiences. While the works of these authors cannot answer the second research question of the current paper, they can provide a valuable perspective on why scambaiters commonly use digital platforms, and what they aim to achieve by doing so.

According to previous research, there are a number of reasons why individuals choose to scambait. Tuovinen and Röning (2007, p. 400) argue that there are at least three different motives, the first being protecting potential victims by wasting scammers' time and resources. The second goal is to gain status and admiration among other scambaiters by outsmarting scammers, and the third one is to seek retribution on behalf of people who have fallen victim to scams in the past, sometimes even the scambaiter themselves or someone close to them. The authors further argue that scambaiting includes an entertainment factor, whether this is seen as a driving force or simply as a bonus (ibid.). Similarly, Sorell (2019, p. 155) claims that scambaiters pursue a type of comic art form. They aim to defraud the scammers in such a way that they eventually start realizing that they have been manipulated, and get increasingly angry (ibid., 165). This strategy has an entertainment value for secondary audiences because the comedic content that the scambaiter uses is an in-joke between scambaiters and their Western followers. It is a type of humor that scammers do not understand (ibid.).

It has become increasingly common for scambaiters to use digital platforms such as YouTube and Twitch to achieve the main goals of scambaiting, as well as entertaining large audiences (Ross & Logi, 2021, pp. 1789-1790). Ross and Logi (2021) researched the interaction dynamics of live scambaiting on Twitch – a live streaming and video sharing platform which is particularly designed for and used by video game players to stream their video gaming sessions (ibid., pp. 1789-1790), while Dynel and Ross (2021) explored Reddit users' communication in relation to scamming and scambaiting on the subreddit r/scambait. Through their analysis, Ross and Logi (2021, pp. 1807-1808) conclude that scambaiting live in front of a large audience successfully coincides with the objectives that scambaiters usually aim to achieve – disrupting the scammers' schemes, discouraging them from scamming people in the future, and educating the public. Twitch live streams add a level of engagement and interaction by allowing an audience to participate in the conversation through comments. The scambaiter can read the comments instantaneously, respond to them, and even incorporate suggestions into their conversations with scammers. According to the researchers, it can also be assumed that the audience's ability to interact with the scambaiter amplifies their enjoyment and encourages them to participate in future scambaiting live streams. Scambaiters' ability to monetize their scambaiting further makes it possible for them to

dedicate more time to it, which in turn facilitates their objectives as scambaiters (ibid.). While Twitch seems to be used mainly because of the opportunity for audience engagement, Dynel and Ross (2021, p. 11) found that many Reddit posts on the r/scambait forum are deceiving in an attempt to be humorous, and often do not adhere to the stated objective of the forum – to share experiences with scammers and scambaiting tactics. The authors further claim that users who post fabricated content do not directly intend to deceive anyone, but they are instead driven by a strong desire to share content that others will find interesting and entertaining. The conclusions drawn by Dynel and Ross (ibid., pp. 12-13) are that Redditors' primary motivation in the r/scambait subreddit is to have fun at the expense of scammers, and that user-generated content should never be taken at face value because of their tendency to fabricate posts.

To conclude, previous research has shown that there are several goals associated with scambaiting, such as keeping scammers from scamming actual victims, gaining admiration from other scambaiters, and educating the public about scams (Tuovinen & Röning, 2007, p. 400; Ross & Logi, 2021, pp. 1807-1808). All of the researchers also concluded that scambaiting includes an entertainment element, which scambaiters achieve through their interactions with audiences on platforms such as Twitch and Reddit.

Theoretical framework

In order to answer the stated research questions and explore how scammers and scambaiters interact with each other, the theories of two different researchers will be applied. Goffman's (1956; 1967; 1974) work on social interactions and performances in which individuals partake will be used to gain an understanding of how scammers, as well as scambaiters, take on personas that are deemed favorable for their desired outcomes. Christie's (1986) definition of the "ideal victim" will serve as a starting point for a discussion on how scambaiters attempt to portray themselves as believable scam victims.

Goffman's theoretical framework

As previous research suggests, scammers must pretend to be someone they are not in order to appear trustworthy and professional in front of their potential victims. Similarly, scambaiters pretend to be unsuspecting victims to deceive scammers. Several theorists have offered their aspects on how someone pulls off this kind of act. Swiss psychiatrist Carl Jung (1967), for example, is known for his theory of the persona. According to him, the persona is a mask that an individual designs and uses to make certain impressions on others, and to conceal their "true nature" (Jung, 1967, p. 190). Whereas Jung focuses on the processes that happen within an individual's psyche, sociologist Goffman (1956; 1967; 1974) instead concerned himself with social interactions and how individuals' actions help them portray themselves in a certain light in front of others.

Goffman (1956) discusses social interaction, and the performances that individuals take part in. He defines performances as "all the activity of a given participant on a given occasion which serves to influence in any way any of the other participants" (ibid., p. 8). According to Goffman, there is a commonly held principle in society that individuals who possess particular social characteristics have a moral right to assume and expect to be treated appropriately by others (ibid., p. 6). This further connects to a second principle: that a person who signifies that they possess particular social characteristics exerts a "moral demand" upon other people, since others are expected to treat and value them in a manner which is appropriate for people of their kind (ibid.). Although disruptions of these principles do occur,

Goffman argues that they would occur a lot more frequently if individuals did not constantly take precautions in order to avoid them (ibid., p. 7).

When an individual puts on a performance to play a certain part, they request their observers to believe that they actually are the "character" they are portraying (Goffman, 1956, p. 10). However, it is according to Goffman also important to consider whether the person believes in their version of reality that they themselves are attempting to portray. One extreme is that the performer is taken in completely by their own act and convinces themselves that their performance is the actual reality. The other extreme, however, is that the performer is not at all taken in or convinced by their own performance. This might be the case if the performer tries to convince an audience only as a means to other ends, since they in that case are not actually concerned with how the audience conceives them (ibid.).

Performances also allow for fabrication – when performers intentionally manage activities to give other individuals the wrong impression of what is happening (Goffman, 1974, p. 83). Although fabrication can be rather benign or even playful, some types of fabrication aim to exploit and harm others for the perpetrator's gain (ibid., p. 103). Goffman (ibid., p. 448) further claims that there are specific conditions which facilitate fabrication in the form of deception. One such situation is when individuals have to rely on a very small amount of information, since this makes it possible for someone to frame the situation differently from reality (ibid., p. 449). Another example of a deception-facilitating situation is one in which an individual is the only available channel of information, and the other individual(s) must therefore rely solely on what that person is saying (ibid., p. 450). Just as an individual can edit what they communicate to others, the same can be the case when audio- and visual material is used to relay information (ibid.).

Goffman (1956, p. 132) uses the term "impression management" to refer to the methods individuals use to avoid disruptions in their performances, and to consciously try to control the way they are perceived. Goffman (1967, p. 9) further uses the term "saving face" to describe people's efforts to maintain a favorable image of themselves in front of others, and to avoid losing face. Losing face, in this context, refers to what happens when individuals feel humiliated or embarrassed due to their inability to meet the expectations in a certain situation (ibid.). Several defensive attributes can be utilized to maintain the performance and "save the show" from disruptions (Goffman, 1956, p. 135). The first is dramaturgical loyalty, which refers to performers' ability to stay loyal to their narrative, without exposing information

which could ruin the credibility of the performance (ibid., pp. 135-136). They must also be taken in enough by their own performance so as to not seem fake in front of the audience (ibid.). The second defensive attribute is dramaturgical discipline. According to Goffman (ibid., p. 137), a disciplined performer is able to remember their part and not involuntarily disclose secrets that could ruin the performance for themselves or for their team. If a disruption does occur, a disciplined performer also has the "presence of mind" to come up with a plausible reason for discounting the disruption, to joke away its importance, or apologize (ibid.).

Goffman's ideas on how individuals impact each other's behaviors in society are shared by several sociologists, both those who lived before him and those who came after. For example, Mead's (1913) theory of the social self is based on the idea that one's "self" is created through interactions with others. Hochschild (1979, p. 558) argues that although Goffman explains how individuals take part in acting performances by managing behaviors, he fails to explain how actors manage emotions. Building on Goffman's and other researchers' theoretical frameworks, she coined the concept of "emotion work", which refers to "the act of trying to change in degree or quality an emotion or feeling" (ibid., p. 561). It is different from emotion control in that emotion work indicates that an individual evokes, shapes, or suppresses an emotion in themselves to portray themselves in a certain manner (ibid.). Hochschild further argues that emotion work is often used by individuals when their feelings do not match the situation they are in (ibid., p. 563). Similarly to how Goffman (1956) and Hochschild (1979) describe how individuals portray themselves in certain ways by performing, Butler (2008) argues that gender is an act. Instead of viewing gender as something a person is, she describes it as a social construct which individuals act out, or perform (Butler, 2008).

The ideal victim

To understand why scambaiters portray themselves as believable victims in their conversations with scammers, it is necessary to first gain an understanding of what a "victim" is in the eyes of society. According to Rock (1986, p. 37), conceptions of morality, danger, and victimization are central to society, since these help to create order and separate "right" from "wrong". Whereas criminals portray moral wrongdoers, society's attitude towards victims relies on its response to criminal actions (ibid., pp. 35, 38). Since people's perceptions

of victimization and crime usually reflect what is conveyed by mass media outlets (ibid., p. 39), one can assume that there might exist an idea of what a "typical" victim is. To answer the present thesis' second research question and investigate why scambaiters take on the roles that they do when speaking to scammers, one first needs to understand their idea of what a typical victim actually is.

Reflecting on victimology, Christie (1986) discusses what he refers to as "the ideal victim". By "ideal", he does not refer to the individuals who are most likely to perceive themselves as victims, or even individuals who are "real" victims of crime. Instead, ideal victims are those who in the eyes of society are most readily given a legitimate victim status when they are exposed to crime (ibid., 18). Christie further lists five attributes which are typical characteristics of an ideal victim:

1. The individual is weak, for example due to age or sickness.
2. The individual is occupied with a project seen as respectable.
3. The individual is in a place they cannot be blamed for being.
4. The offender is bad and big in relation to the individual.
5. The offender has no personal relationship with the individual. (ibid., 19).

As an example of an individual who possesses all of these attributes, Christie paints the picture of "the little old lady on her way home in the middle of the day after having cared for her sick sister" and who is "hit on the head by a big man who thereafter grabs her bag and uses the money for liquor or drugs" (ibid., 18-19). Christie argues that ideal victims both need and create ideal offenders (ibid., p. 25). The more ideal the victim is, the more ideal the offender is, and vice versa (ibid.).

Although Christie's theory on ideal victims has been highly influential and important in victimological research, some researchers argue that it needs to be modified or updated to be applicable to modern society's opinions on who a victim is. Bosma et al. (2018, p. 38) argue that although there still seems to be a need for victims to possess ideal characteristics to be considered victims, these characteristics do not only depend on the victimized person and their relationship with the offender, but they also depend on the context and the observers' motives. Nafstad (2019, p. 4) further discusses that women have different positions in today's society than they had 37 years ago when Christie wrote his article. Christie (1986, pp. 20-21) himself discusses how female victims of domestic abuse were "not yet" perceived as ideal victims, but how he could see development moving in the direction of allowing these women

legitimate victim status. Nafstad (2019, p. 4) further notes that Christie's prediction is now fulfilled to some extent, particularly considering the criminalization of domestic violence and the development of laws on it.

Cross (2018) compared Christie's (1986) list of attributes one must possess to classify as an ideal victim to online fraud. She found that although online fraud victims fit into some of the characteristics, they overall fail to qualify (Cross, 2018, p. 256). The main reason for this is that they through their actions are considered active contributors to their own victimization, for example by being on the Internet (ibid.).

Although Christie's theory of the ideal victim might not be perfect in terms of encompassing all types of victims, it can still offer important insights into which individuals are most readily seen as actual victims by society, and which traits these victims typically possess. These can in turn help explain why the scambaiters might try to present themselves in a certain manner when pretending to be victims.

Performance theory and the ideal victim

Even though Goffman's (1956; 1967; 1974) theoretical standpoint and Christie's (1986) victimological concept seek to explain different phenomena in the social world, they also share some similarities. Both Goffman's theory of performances and Christie's concept of ideal victims emphasize the role that social expectations play in shaping an individual's identity and behaviors. Whereas Goffman's theory suggests that individuals put on different fronts that are designed to meet the expectations of other people, Christie's definition of the ideal victim indicates that victimized individuals have to adhere to specific cultural scripts in order to be socially viewed as legitimate victims who are deserving of society's sympathy. Both frameworks further touch upon power dynamics within social interaction. Discussing Goffman's theoretical framework, some people have more control over how they are perceived than others, for example people who possess authority or social status. Similarly, Christie's definition of ideal victims implies that individuals who are marginalized or lack social power may struggle when it comes to being recognized as legitimate and credible victims. Also, both concepts stress the significance of social contexts when it comes to shaping individuals' identity and perception. Goffman's performance theory explains how individuals create meaning in specific social contexts, while Christie's concept of the ideal

victim highlights how cultural narratives affect the way we understand victimhood and who qualifies as a victim. Both of these concepts will be used in the present study to help gain an understanding of how and why scammers and scambaiters portray themselves in certain ways when playing their respective roles during conversations.

Methodological framework

This section of the paper will present the methodological framework by first providing a description of the setting and population, followed by a discussion on data collection, and the method used for the data analysis. Further on, the methodological limitations will be acknowledged and lastly, there will be a discussion on the ethical considerations.

Since the purpose of this thesis is to gain an understanding of the deceptive performances of scammers and scambaiters during their conversations, videos from scambaiting YouTube channels were used as the main material, combined with scam descriptions from online forums. These were then analyzed using a narrative thematic content analysis.

Choice of data: online videos

In order to gain an understanding of how scammers attempt to trick their victims and how scambaiters portray themselves as believable victims, it is necessary to get access to conversations between scammers and scambaiters. As mentioned by previous researchers (Dynel & Ross, 2021; Ross & Logi, 2021), scambaiters often use internet-based platforms to educate and entertain the public. Several scambaiters use YouTube to record and post videos of their conversations with phone scammers. The videos that these YouTube channels post offer a unique insight into how conversations with phone scammers typically play out, since real victims do not usually record their phone calls with scammers and post them publicly. This rare opportunity to be able to actually hear what scammers tell "victims" during their phone calls, and how scambaiters might respond, is the reason why scambaiter YouTube videos were used as the primary data for this thesis.

More specifically, the primary data consisted of videos from six different scambaiter YouTube channels. These channels all have varying numbers of subscribers ranging between 32 thousand to almost 5,5 million. They all post videos regularly, and some also host livestreams where they call up scammers in front of a live audience. Several of the scambaiters use different "characters" when speaking to scammers, sometimes using a voice changer to sound like a person of a different age, gender, nationality, or a combination of these.

Data sampling

Seeing how there is a very large number of scambaiter YouTube channels which all post substantial amounts of content, a purposive sampling technique was applied to select videos that possessed certain characteristics and were deemed relevant for the purpose of the research (Etikan et al., 2016, pp. 2-3). 10 videos in total were used, with the first criteria being that they all had to be over 40 minutes long. The reason for this is that shorter videos are often too cut down and edited to get a complete picture of how the conversations play out. Some scambaiting YouTube channels had only posted shorter videos containing the "funniest" parts of their phone calls with scammers, and therefore, these channels were excluded from this thesis. The second sampling criteria was that the videos must contain enough footage of the different parts of the scams, to get a general picture of how the scams play out. Even the videos that were over 40 minutes long were still often shortened and edited by the owners of the channels, which is why a few recorded live streams were also used as a complement. In the end, seven edited videos and three live streamed videos were used for this thesis. Whereas the edited videos were all between 42 minutes and 1 hour and 15 minutes long, the live streamed videos were between 2 hours and 13 minutes and 2 hours and 55 minutes long. Although the chosen videos might not be generalizable in that they describe how every scam plays out, they aim to capture how a scam might transpire and what techniques scammers and scambaiters might use to try to trick each other. As Ellis (2020, p. 82) argues, qualitative research does not necessarily need to find generalizable answers, it "seeks to show findings which are representative of the population under study". Experiences are personal, and with the huge number of scams that exist today, it is impossible to get a comprehensive overview of all of them. Similarly, different scambaiters might use different methods to trick scammers and portray themselves as victims.

A selection of scam descriptions from several different online forums were also used as a supplement to the YouTube videos. These were selected through a purposive sampling technique, the criteria being that they had to contain descriptions of how the scams played out, and preferably also something about the scammers' persuasive techniques. 22 discussion forum posts ended up being selected from a number of different online forums such as Reddit, MSE, and Silversurfers. The posts were all found through Google searches or searches directly on the forums. All of the posts were written by individuals who described scams that they or a close family member had been exposed to. Although the people on these forums did

not describe the scams down to every detail, they still offered a general overview of how real scams might play out. Apart from acting as a supplement to the scambaiting YouTube videos, these written descriptions further offered personal accounts of scams from actual victims' perspective, which is valuable from a validity aspect when researching the techniques that scammers might use to manipulate victims.

Aside from the mentioned YouTube videos and online forum posts which were ultimately selected for this thesis, many more accounts were watched and read through during the selection process. These have offered additional insights into the subject and aided an immersion into the data, as well as having informed the interpretations made in the analysis. However, this material has not been systematically analyzed.

Analysis

All of the videos were first transcribed using the video editing and transcription program Descript, and the transcriptions were then compared with the videos and corrections were applied where the program had not transcribed correctly.

In order to analyze the data and answer the research questions, a combination between a thematic content analysis and a narrative analysis was applied. Thematic content analysis is a method which aims to identify and analyze themes within data (Braun & Clarke, 2006, p. 6). For the purpose of this thesis, all video transcripts were coded to find themes within the phone calls between scammers and scambaiters. The goal with coding is to find themes which reflect the material as a whole (Anderson, 2007, p. 1). The transcripts were first read thoroughly, which gave an idea of how the scam calls transpired and which techniques were frequently used by scammers as well as scambaiters. In the second stage, they were read through again while highlighting important sections and putting them into categories. While coding, different themes emerged. As Braun and Clarke (2006, p. 10) argue, what counts as a theme is something that captures important aspects in relation to the research questions. In a third stage, these themes were revisited and while some stayed as they were, others were broken up into sub-categories. The themes were divided into two categories – themes related to the scammers' techniques and narratives, and themes related to the scambaiters techniques and narratives. Examples of themes related to the scammers' techniques are: "scammer making the victim feel safe", "scammer playing the hero", and "scammer using kindness/flattery",

while examples of themes related to the scambaiters' techniques are: "scambaiter entertaining the audience", "scambaiter asking for help", and "scambaiter questioning the scammer". The finished themes which emerged from the coding of the material were then analyzed using the theoretical framework – Goffman's performance theory and Christie's concept of ideal victims.

As a supplement to the thematic analysis, narrative analysis was used to divide the material into different sections and analyze their content as well as how they related to each other (Johansson, 2005, pp. 279-280). More specifically, the analysis was based on what Riessman (2005, p. 5) refers to as performative analysis. It is an analytical approach in which storytelling is viewed as a performance that aims to move and persuade the audience (ibid.). As Riessman (ibid.) further argues, the focus lies on aspects such as how the characters are portrayed and positioned, which setting the story is performed in, and how the conversation between the actors is enacted. The analysis was divided according to the dramaturgical parts of the phone conversations between scammers and scambaiters. Starting with the introductory part of the conversations and then continuing on with the middle part and the resolution, the scammers' and scambaiters' techniques and performances were discussed and analyzed.

Methodological limitations

Because the purpose of the scambaiting videos is partly to serve as entertainment, it is impossible for viewers to guarantee that the conversations between the scammers and scambaiters are real and not staged. As Dynel and Ross (2021) found, many scambaiters on platforms such as Reddit make up stories in order to be entertaining. Additionally, the scammers add conversational elements purely for entertainment purposes, which obviously do not occur in normal conversations between scammers and real victims. However, for the purpose of this research, scambaiting videos from six different YouTube channels were used, which increases the chances of material resembling ordinary exchanges between scammers and their victims. Despite the mentioned disadvantages, scambaiting videos allow researchers an insight into how scams play out which is difficult to come by otherwise. In particular, the videos offer unique insights into the way scammers communicate with victims. The ideal situation when researching scammers' techniques would have been for the researcher to speak directly to scammers. However, this method entails many ethical problems including possible

dangers for the researcher, since it is difficult to pretend to fall for a scam without risking actually losing money or accidentally sharing personal information. Furthermore, many scambaiters are skilled in using programs and methods which makes it look like they provide the scammer with personal information or banking information, even though they are not. For example, some scambaiters have found methods to hack scam call centers and use their own tools against them, which has even led to scammers being arrested (Mujezinovic, 2022). Multiple scambaiters further have backgrounds in programming which equips them with knowledge about what precautions to take (ibid.).

In order to increase the chances of scam phone calls from the scambaiting YouTube channels reflecting real phone calls that victims might get from scammers, the material was compared with descriptions of scams from online forums. Although the scambaiting videos contain much more information on how the scams play out, the online forum posts were used to get a general idea of common scams and their techniques.

Ethical considerations

The first step in qualitative research ethics is informed consent, which refers to providing information about the research to the participants and letting them decide whether or not they want to take part in the research (Wiles, 2013, p. 25). However, since this thesis investigates public material in the form of YouTube videos and discussion posts on public online forums, it is near impossible to get informed consent from everyone involved. Since the owners of the YouTube channels post their content on a public platform where they have thousands, and sometimes millions, of subscribers, it seems relevant to assume that they are comfortable with their material being seen and spread by the public. Many, if not all of them, even want their videos to be spread and seen by as many people as possible. One scambaiter whose videos were used for this thesis cooperates with American Association of Retired People to spread awareness about scams, for example (Tait, 2021). However, although they may be viewed as public figures, the names of the scambaiters and their YouTube channels have been kept anonymous in this thesis.

The second group of participants, the scammers whose voices can be heard in the videos, are impossible to collect informed consent from since their identities are not known. Because they are anonymous, however, the risks of them suffering harm because of this research are

extremely slim. The third group of participants, the anonymous posters on online forums, are also challenging to obtain informed consent from. However, these individuals will remain unnamed and no personal information about them has been used for the purpose of this research. According to Wiles (2013, p. 36), it is not necessary to ask for consent when using material that has been posted to online environments that are seen as "public". Moreover, this research is not focused on individuals but on sociocultural patterns of communication.

Another important ethical consideration to make when conducting research where public, web-based data is used is that the information obtained from the YouTube channels and online forums is used in a responsible and non-misleading manner. Although it is necessary for the researcher to interpret the material to a certain degree, information should not be taken out of context or misinterpreted. It is also important that the researcher's own preconceptions and opinions do not influence the way that the material is used and analyzed. I, as the researcher, have therefore done my best to put my own opinions and biases aside in order to remain an objective interpreter of the material.

Results

Scammers' performances and techniques

The following section of the paper will discuss the most significant findings and analyze them in relation to the main theories and concepts. The material will also be compared to findings of previous research on scamming and scambaiting. This section will consist of two main chapters. The first chapter will focus on the scammers' performances and manipulation techniques, while the second chapter will concentrate on the scambaiters' deceiving performances and how they portray victimhood during their conversations with scammers. Each chapter will be divided into sub-sections which describe and analyze the different components of the phone calls between scammers and scambaiters.

So, this chapter focuses on answering the first research question: How do scammers verbally manipulate their potential victims through phone conversations? The techniques that the scammers use to manipulate and exploit their "victims" in the YouTube scambaiting videos will be described and analyzed using Goffman's (1956; 1967; 1974) theoretical framework and concepts. The chapter will be divided into three sections which focus on the scammers' performances in the beginning, middle, and end parts of the conversations. Although the "victims" in these videos are all scambaiters, they will be referred to as "victims", since this section focuses on the scammers' performances which they put on for individuals who they believe to be actual victims.

Beginning

In the scambaiting YouTube videos, the scams had typically been introduced through a pop-up on the victim's computer, indicating that their computer had a virus and providing a phone number for the "victim" to call and get help with solving the issue. In other cases, the "victim" had received an email telling them that they had been charged for the purchase of a certain service or product, and to call customer support if they wanted to cancel this purchase. These seemed to be common introduction tactics in the scam descriptions from online forums as well. One user posted the following description on the Reddit forum r/AskReddit under the thread "How to get rid of a tech support scam?": "It all started in a scary pop-up that looked

exactly like it was from Microsoft." Once the potential "victim" decides to call the number or follow other instructions from the pop-up or email, the scam begins.

The introductory part of the scam call is of great importance to scammers, since it is the part where they begin their performance and set the tone for the rest of the conversation. In all of the YouTube videos which include the beginning of the conversation, the scammer started off by introducing him/herself with a simple introductory phrase such as: "Thank you for reaching PayPal. This is Jennifer. How can I help you today?" (Video 1). Just like Lester et al. (2020) found in their research, the scammers in the scambaiting YouTube videos all introduced themselves with English-sounding names such as "Jennifer", "Ryan", or "Andrew", while speaking with an accent that was typically Indian-sounding. After the first introductory phrase, the scammers in the videos typically continued to speak with very professional voices, while referring to the "victim" as "sir" or "madam". "Jennifer" looked up the "victim's" invoice number, and then informed him that a purchase had been made on his PayPal account: "Sir, as I can see there is a purchase made on PayPal. So, are you the one who has made this purchase for Bitcoin?" (Video 1). By speaking with a calm and professional voice, the scammer projected an image of herself as a competent and experienced customer support-worker. As Goffman (1956, p. 6) argues, individuals who possess certain characteristics have a right to expect to be treated appropriately by others. By playing the part of a professional customer support worker, "Jennifer" invited the "victim" to treat her as such, and hopefully follow her instructions.

After being informed by the "victim" that he did not make the purchase, "Jennifer" used one of the methods found by Shaffer (2012): she pointed to the urgency and seriousness of the situation, while simultaneously using kindness and trying to build a trusting relationship, which is illustrated in the following quote: "Then if you are not the one, sir, who did this, then some third person is trying to misuse with your personal information, like by creating a fake PayPal account under your name, like your identity has been compromised." (Video 1). Her voice remained kind and calm while she tried to instill fear in the "victim" by telling him that his identity had been compromised. Similarly, a social security scammer who introduced himself as "Sean Brown" attempted to assert authority by stating that he is an "investigative officer", disclosing his alleged badge number, and then using a scare tactic on the victim:

I'm extremely concerned about the situation because right now, I'm

> not sure whether you're aware about this or not, but we have some illegal activity that has been done with the help of your social, and there are three allegations which are highly, extremely sensitive and non-tolerable criminal activities that happened with the help of your personal information. (Video 8).

By portraying himself as an authoritative person of power and then claiming to be "extremely concerned" about the "victim's" situation, he attempted to make the "victim" concerned as well. By taking on the role of an "investigative officer", he did what Goffman (1956, p. 6) describes as exerting a moral demand upon the "victim", since the "victim" was then expected to treat him as someone to be respected and trusted. If a powerful officer is worried about the situation, then the "victim" will likely feel that it is appropriate for them to be worried as well.

Another common theme that could be found in several of the YouTube videos was that the scammers insinuated that the victims were at fault for the issues they were experiencing. This was especially common in two types of scams which occurred in the videos: the technical support scam and the social security scam. The scammers usually did this after having established the alleged issue and providing the "victims" with worrying information, such as their personal information having been stolen and used maliciously. An example of a scammer suggesting that the "victim" was at fault can be found in the following example: "Because, sir, this infection which you have, that can come into a computer only in [sic] two conditions. Either you have clicked on the wrong link, or you have downloaded something." (Video 7). By suggesting that the "victim" has caused the problem, the scammer then reached a point in his performance where he portrayed themselves as the potential hero capable of fixing the "victim's" mistake. The following quote is an example of this:

> So that we can help you block the third person who is trying to misuse your personal information. Then we will be guiding you, like you need to fill a cancellation form from your end. Then we will be canceling this purchase and if there is any deduction from our end, then we will be providing you with a refund amount. Alright? (Video 1).

Following Goffman's (1956) argument, the scammer playing the role of a hero places an expectation on the "victim" to be grateful and follow the instructions of the hero, since that is what is socially expected from someone who is faced with a serious problem and receives an offer of help. To further make the "victims" feel safe and trusting, the scammers used words and phrases which pointed to the idea that the "victim" is in a safe space, which Whitty (2013) also found in her research on online dating scams. For example, the scammers in multiple videos kept repeating to the "victim" that they were connected to "a secure server" (Video 2; Video 4; Video 7), "a secure connection" (Video 1) or "the secure line of Microsoft" (Video 3), while continuously telling the victim not to worry because they are going to fix their problem. Although this entire performance is a fabrication designed by the scammer to get money, the "victim" has no choice but to act upon the information they receive. In this case, the scammer is the only source of information apart from the pop-up or email the "victim" received prior to the conversation, which according to Goffman (1974, p. 450) makes it easier for the fraudster to frame the situation differently from reality without the "victim's" knowledge.

As previously mentioned, the introductory parts of the scam calls are crucial for scammers to establish relationships with their "victims", which can potentially increase the chances of successful scams. Throughout the beginning of the conversations, the scammers stayed calm and spoke with kind voices and language. While all of the scammers in the videos displayed signs of wanting to establish some sort of relationship with the "victims", they had different ways of going about this. Some seemed to want to establish a strictly professional and authoritative relationship. An example of this was the social security scammer in video 8, who quickly set a professional tone which he tried to keep throughout the rest of the conversation. However, several of the scammers in the videos instead started off their performances as professional, but soon switched to attempting to establish more personal relationships with the "victims". This commonly happened after the "victim" told them something which the scammer realized they could use in their performance to hopefully initiate a more friendship-like relationship. An example can be found in video 9 after the "victim" told the scammer that her husband had passed away:

> So your husband, he paid to us like $399 to us like three years ago.
> That amount will be refunded to you back. We're going to help you to

> release your refund amount back to you. Okay? Mr. Richard, he used to, uh, he used to do the same thing with me. (Video 9)

The scammer in this video used the information he was given by the old woman against her, to win her trust and make her more likely to comply with his instructions. Since the husband in this scenario had passed away, the "victim" was put in a situation in which Goffman (1974, p. 450) claims it is easier for the scammer to lie unnoticed, since the "victim" could not verify the information with anyone else. The scammer created a fabrication in which there was a reasonable explanation for the money deduction on the "victim's" account, and in which he was the sole source of information. He also claimed to have spoken to Richard, the "victim's" husband, to further appeal to their relationship and seem more trustworthy. This personal connection that the scammer attempted to make can be interpreted as the beginning of the "grooming process", which Whitty (2013, p. 23) discusses in her research on online dating scams. The scammer fabricated a seemingly safe and friendly environment to make the "victim" feel comfortable. It is also in line with Shaari et al.'s (2019) research, which shows that scammers often use politeness strategies early in their scam calls, such as claiming common ground and finding similarities between them and their victims. In this case, the "victim's" husband served as a factor which they had in common, since they both had a relationship with him.

Some of the YouTube videos did not include the scambaiters' and the scammers' first contact with each other since they seemed to have already spoken earlier, usually the previous day. The conversations in these videos typically consisted of more friendly language, as the initial relationship had already been established prior to the conversations depicted in the videos. An example of this can be found in video 6, where their conversation indicates that they had been speaking the previous day:

> Scambaiter: Is it- this was Peter Parker?
>
> Scammer: Yeah, madam. Peter Parker. And I hope you remember. So first you need to just make your computer on. Okay? Take your time.
>
> Scambaiter: Okay. Because- yeah. Okay.

> Scammer: And I call [sic] you several time, madam, and I'm just thinking about you. What happened? (Video 6)

Like the argument made in Shaffer's (2012) research, the scammer conveyed a personal connection as a persuasion strategy. The scammer, "Peter Parker" kept reminding the "victim" of their familiarity with each other during the beginning of their conversation to make her feel safe and more likely to follow his instructions. He also played the part of someone who cares about the "victim" and is concerned for her wellbeing, by saying "I'm just thinking about you" and asking her what happened the previous day. This can also be interpreted as a manipulation tactic. The scammer signified that he is a kind and caring person, which according to Goffman's (1956, p. 6) argument puts the moral demand on the "victim" to view him as such, and hence treat him as someone who can be trusted on behalf of his kind-hearted character. As Shaffer (2012, p. 168) further found, some scammers use flattery early in the conversations to further evoke positive emotions within the victim towards the scammer. An example of this technique can be found in one video, where the scammer told the "victim" the following: "How are you? Your voice is very lovely, actually." (Video 6). After they had exchanged a few more sentences and the "victim" told the scammer that she is 79 years old, the scammer proceeded to say: "My god, your voice is very lovely. I was thinking like it was a 26-year-old." (Video 6). By complimenting and flattering the "victim", the scammer presumably hoped that she would continue talking to him with a positive attitude, so that the scam could proceed as planned.

Scam escalation and problem encounters

After the initial introduction, the scam continues as the scammer starts to ask for access to the "victim's" computer, and ultimately, for money. In the scambaiting YouTube videos, almost all of the scammers asked the "victim" to download a remote access program, for example AnyDesk or TeamViewer, which would allow them to gain control of the "victim's" computer. In the cases of technical support scams, the scammers usually justified getting remote access to the "victims'" computers by telling them that they were going run a network scam, whereas the refund scammers guided the "victims" through it as a necessary step to them getting their money back. Asking the victims to download a remote access program was

a common tactic in the scams described on online forums as well. For example, one user posted the following to the MSE forum under the thread "Scam phone calls":

> I have today had a new series of scam phone calls saying the usual that someone else is using my home hub but this time a new phrase has come in with them asking me to go to Google and type 'Teamviewer' (MSE, "Scam phone calls")

After securing remote access to the "victims'" computers, the scammers in the videos used different methods to further convince the "victims" that they needed their help to solve the issues they were allegedly experiencing. In the case of technical support scams, the scammers in some of the videos used the information they found on the "victims'" computers to promote their narrative. In video 7, the scammer showed the "victim" a fake pop-up to prove that his computer has been affected by a "spyware attack":

> Sir, it is a spyware attack. Please see, I told you, by these error numbers. This is five things, okay? […] It, it's infected the virus since [sic] five years and the following information has been stolen. These are the four information [sic] which has been traced out: Facebook, credit card, email and photos. Do you use any of these information [sic] on this internet network? (Video 7)

As Goffman (1974, p. 450) argues, audio and visual material can easily be used to manipulate information and make fabrications possible. In multiple videos, the scammers utilized pop-ups or websites containing false information to convince their "victims" and uphold their deceiving performances. They then proceeded to tell the "victims" that they were doing a network scan to check who is currently connected to their network. The scammer in video 7 explained the following:

> It'll scan each and every device which you have on this internet network. It can be a smartphone, tablet, iPad, iPhone, any computer,

> even a wireless printer. So, the devices will be scanned. […] And by this scan, we are checking your active connections. All the active devices on the internet network are getting scanned. (Video 7)

The scammer continued to instill the "victim" with a false sense of security by assuring him that they were checking his entire internet network to find issues. He then proceeded to attempt to evoke fear and concern within the victim by telling him that his IP address had been "infected" and that hackers were using it:

> […] your IP, which you were using earlier, now somebody else is using it, and they have provided you a new IP so that at least you can use the internet. And on that infected IP, there are different people connected. And they're established. That means they can see your screen, they can see what information you have, what things you are doing, which site you're searching. And even if they want to transfer something from your computer to their computer, sir, they can easily do that. (Video 7)

Many of the scams portrayed in the videos – but especially the technical support scam – largely depended on the "victims" being rather unskilled when it came to computers and technology in general. An individual who possesses knowledge on technology would first of all realize pretty quickly that what the scammer is trying to tell them is not true, and second of all, likely feel like they could tackle problems such as viruses themselves, without the help of a "technical support worker". Some of the online forum users also seemed to have noted that it is highly beneficial for scammers if the potential victims are elderly and/or lacking computer skills: "I work for a phone company and this shit is real. I see it all the time. They target elderly people (mainly women who live by themselves and no, I don't know how they find out this info)" (Reddit, r/AskReddit). After convincing the "victim" that their computer had become victim to spyware, hackers, or a virus, the scammer offered the solution – a security software which they could install on the "victim's" computer for a certain amount of money. In video 7, the scammer offered the "victim" the following security solutions:

> All right. Now I'll be showing you both the options, sir. Either you can take the network protection, that is the server security, or you can take the computer security. You have both the options. I won't be forcing you for any of them. But I'm suggesting you that you take the big proper server security because that is something which will protect all your devices along with the network. (Video 7)

This is a deciding part of the scam for the scammer, since it is his first opportunity to actually get money from the "victim". The purpose of the entire conversation prior to this moment was to make the "victim" more prone to pay. By having created a relationship and evoking feelings of concern in him by making him feel like his issue was too severe for him to solve by himself, the scammer likely hoped that the "victim" felt like the best option for him would be to buy the scammer's services. The scammer further presented the two security options in such a way that the "victim" does not feel forced to purchase the services. However, he still made his own recommendation, probably hoping that the victim would follow his advice and buy the more expensive option.

When it came to the refund scams, scammers created fabrications by using manipulated visual material to make it look like the "victims" were receiving the refund amount on their accounts, even though no money had actually been transferred. As explained by the scambaiter in video 9, the scammers commonly achieved this using the remote access program to hide the screen from the victim, and then changing the HTML on the bank account to make it look like money has been added. Other times they transferred money from the "victim's" savings account to their checking account. This is where the refund scammers usually introduced a problem into their narratives. They made it look like the "victim" was refunded too much money, typically by adding another zero at the end of the refund amount. In the videos, the scammers generally explained to the "victims" that there had been a technical error, or that they had made a mistake and accidentally transferred too much money. An example can be found in the following quote:

> See, I made a huge mistake over there, right? Because while I'm talking to you, right, and I'm thinking about Richard and while I'm- I have by mis- accidentally, I have put it too many zeros over there.

> And instead of a thousand dollars I have given you a hundred thousand (Video 9)

The scammer then proceeded to tell the "victim" that she needed to pay the money back, since it was all a mistake. By creating a fabricated scenario in which he made a mistake that the "victim" has to solve, the scammer switched his performance. Before, he had been the "hero" capable of helping the old lady with her problems, but with the introduction of this "mistake", he instead flipped their roles. At this point, he became the one in need of help, while the woman had the opportunity of becoming the hero. This narrative seems quite uncertain for the scammer, since it relies on the "victim" being willing to do the "right thing" and send the money back. It seems likely that the scammer's and "victim's" relationship plays a very important role in this situation, since one can assume that it would take less convincing if the "victim" has positive feelings towards the scammer. When explaining why the mistake was made, the scammer mentioned the woman's husband, Richard, and implied that he got distracted when thinking about him, which can be interpreted as an attempt to seem empathetic and kind-hearted. It could further be an attempt to evoke an emotional response in the "victim", to make her more willing to help solve the problem. Using Goffman's (1956) ideas on social exchanges, it is likely that if someone acts empathetically and kindly towards an individual, that individual responds by acting in a similar manner. As Goffman (ibid., p. 7) further argues, the social norm of treating someone appropriately in relation to how they portray themselves is not often broken, since most people make an effort to uphold it. It does, however, occur. In video 10, the scammer played the role of a PayPal customer support worker who spoke to a "victim" whose account had been charged for something he did not purchase. The scambaiter purposefully acted rude to the scammer, seemingly without reason. After being told by the "victim" that he was going to rate him only "one star", the scammer said the following: "See, you are the boss. I'm working for you. I'm doing things, whatever you are telling me to do, but you won't appreciate me." (Video 10). The scammer played the role of a professional and helpful customer support worker who was trying to help the "victim" and seemed frustrated when the "victim" did not respond to him accordingly. By portraying himself as helpful, he requested appreciation which he felt that he had deserved. The lack of this hence led to the scammer projecting the impression that he had been unfairly treated.

After presenting the “victims” with the issue of them having accidentally received too much money, the most important part of the refund scam commenced. It would be revealed whether the scammer had managed to convince the “victim” to go out of their way to pay the money back or not. This was a more complicated process than expected, since the “victim” could not simply transfer the money back to the scammer’s bank account. Instead, the scammers in the videos asked the “victims” how close they were to a convenience store like Target, Walmart, or BestBuy: “Can you tell me, like do you have any Target store close to your place?” (Video 4). When the “victim” answered that they did, the scammer continued giving them directions: “So what you have to do is, you have to go to the Target store, and you have to buy two Target gift cards worth 2000 dollars each, okay?” (Video 4). The request to buy gift cards as a mode of payment occurred in most of the YouTube videos portraying refund scams. The scammers gave the “victims” clear instructions to follow when driving to the store, which could sound something like this:

> Talk to me while you’re driving, okay? You just have to leave your phone as it is. Do not, you know, hang up the phone. I’ll stay on the line and you can drive. You do not have to talk to me while you’re driving, okay? Only when you reach the parking lot of the Target store you let me know, and I’ll talk to you then, okay? (Video 4)

After the “victims” told the scammers that they had arrived at the store, the scammers continued giving instructions which they were very insistent that the “victims” should follow. In video 4, the scammer presented the following instructions:

> Scammer: Now what you have to do is you have to walk inside the store and you have to go to the store and you have to tell them that you want to buy two Target gift cards. If they ask you for what purpose are you buying the gift cards, what will you tell them?
>
> Scambaiter: For the internet?
>
> Scammer: No, not for the internet. If you tell them that you're buying the gift card for a, you know, commercial or a business purpose, they

> will charge you a tax. […] So simply tell them that you're going for a marriage ceremony. Right? So you're buying two cards. Tell them that you are going for a marriage ceremony. (Video 4)

The scammer understood that if the "victim" had told the store clerk that she was buying gift cards to refund money back to a customer support worker, they would instantly know that she had been exposed to a scam and inform her. Hence, he instead asked her to lie and say that she was buying the gift cards as a wedding gift. Considering that the scammers' requests involve the "victim" having to drive to a store to buy the gift cards, it is not a small favor to ask. So how did the scammers manage to convince the "victims"? Various techniques were used in the videos, depending on how willing the "victim" seemed to be to follow the instructions. In video 5, the scammer told the "victim" that a technical error caused her to be refunded too much money, and then asked her if she could do him a favor. When she answered that she probably could not, since she was "a little busy tonight" (Video 5), the scammer responded the following: "Okay. But if you don't, madam, I will lose my job." (Video 5). This strategy seemingly aimed to plead to the "victim's" conscience and make her feel guilty for potentially causing him to lose his job. Methods which supposedly aim to make the victims feel guilty could be found within the scam descriptions from online forums as well. This is described in the following post from the Reddit forum r/AskReddit as an answer to the question: "Serious: what scams have you fallen for?":

> "I told them I wanted to call them back the next morning (because I wanted to call my ISP back and ask what the fuck was going on), and the guy tried to guilt trip me into staying, claiming they had all stayed after hours just for me and "you really don't have just 5 minutes?" and blah blah blah." (Reddit, r/AskReddit)

The scammer in the description seems to argue that since he has dedicated time to "help" the victim, there is an expectation on the victim to repay the favor. Although all of the scammers in the videos shrewdly used what Goffman (1956) refers to as impression management to consciously control how they were perceived, the scammer from video 9 also displayed presence of mind when trying to convince his "victim" to follow his instructions. Throughout

the conversation, he proved that he is observant by listening to what the woman was telling him and responding accordingly. The "victim" played a song for the scammer and told him that her husband, Richard, wrote that song before he passed away. When she asked the scammer what he thought the song was about, he answered the following:

> See there is something in his heart, right? He is saying that this is not right, that you need to- you are not supposed to keep someone's funds in your account. You have to send that money back to the person and from where you have received the money, right? (Video 9)

The scammer tried convincing the "victim" by making her feel like paying back the money was what her husband would have wanted her to do. He knew that her strong loving feelings towards her late husband could cloud her judgment, and hoped that she would choose to honor her husband's wishes. Another technique used in the videos, especially in the social security scam, was intimidation and threats. Similarly to what Lester et al. (2020) found in their research, the social security scammer "Sean Brown" intimidated the "victim" by telling her that crimes had been committed using her personal information, and that unless she cooperated, he was going to send the police to arrest her. When she started getting scared and stressed, "Sean Brown" told her the following:

> I understand, Wang, but you need to also understand that right now if you panic too much, if you are in a lot of stress, you will make some mistakes. And mistakes will be counted, and if anything goes wrong, we will have to send the police to arrest you. I want you not to get arrested for that reason. That is the reason why I'm telling you to calm down and act smart. Okay? (Video 8)

By continuously telling the "victim" that she would face serious legal consequences if she did not follow his instructions, the scammer presumably hoped to keep her frightened enough so that she would comply with his requests. At the same time, he told her that if she only follows his instructions correctly, everything would be okay since he trusted that she had not committed the crimes and wanted to help her. This narrative suggests that while he played the

role of the potential hero who could save the "victim", he is also someone who could potentially be dangerous to her and who should therefore be respected.

Resolution

After the scammers in the videos requested money from their "victims", the results were varying. Whereas some of the scambaiters tried to keep the scammers occupied by, for example, pretending to drive to the store and buy gift cards only to get back home and redeem them themselves, others did not manage to keep the scammers on the line without actually giving them money, or the scammers realized that they themselves were being "scammed". A common theme which occurred in multiple videos was that towards the end, the scambaiters started to test the scammers by questioning them and sometimes even confronting them directly. As Goffman (1956, p. 135) argues, individuals frequently use impression management to avoid disruptions to their performances, but also to save the show once disruptions do occur. Being questioned by the "victim" can in this case be interpreted as a disruptive situation in which the scammers need to use their impression management skills to save the show. Dramaturgical loyalty, the first defensive strategy which Goffman (1956, pp. 135-136) discusses, was exhibited by several of the scammers in the videos when questioned by "victims". In video 8, the "victim" questioned the scammer, "Sean Brown", after he claimed to be in Texas, since his accent did not sound American. Their conversation played out as follows:

> Scambaiter: How long have you been living in Texas? Right? You like- you were born there or what?
>
> Scammer: No, no, no, no. And sir, this is, look, I don't want to be rude, okay? But we are not- there is nothing personal between me and you. Everything is professional. So, right now it's okay if you want to talk to me about that. I was not born in Texas. I was born in New York. My mom is half Jewish and my dad is African American. So, I believe you understand by my accent, it's like a little bit American and African, correct? (Video 8)

The scammer, “Sean Brown”, stayed loyal to his narrative and refused to disclose any secrets which could ruin his performance. In a situation where he could have easily risked losing face which according to Goffman (1967, p. 9) can lead to embarrassment, he managed to save face by answering the question while also insinuating that he would not be answering any more personal questions since his relationship with the “victim” was strictly professional and authoritative. His voice further remained calm and professional when answering the question, showing that he was capable of keeping his composure even when his performance was threatened. Additionally, “Sean Brown” displayed what Goffman (1956, p. 137) refers to as dramaturgical discipline, since he had the presence of mind to be able to come up with a plausible explanation when questioned. Although several of the scammers in the videos were able to keep calm and come up with plausible answers when challenged, not all of them displayed this dramaturgical discipline. In video 1, the scambaiter questioned why the scammer told him that she was going to cancel the services from her end, when this was obviously a lie:

> Scambaiter: You're telling me the truth. Why do you say this?
>
> Scammer: What is that? What are you saying? I can't understand.
>
> Scambaiter: Oh, you can't understand. So you don't understand what I'm saying?
>
> Scammer: No, I can't. (Video 1)

The scammer did not seem to know what to answer in order to save the show, so she simply pretended she did not understand what he was asking her instead. However, she might have already understood that the “victim” had realized that it was a scam or that he was actually a scambaiter, and therefore found it unnecessary to try to come up with an explanation since it was nearly impossible to save the scam at this point. Shortly after this interaction, the scambaiter told the scammer that he knew their call center is located in Pune, a city in India, and the scammer briskly hung up the phone.

According to Goffman (1956, pp. 135-136), a dramaturgically loyal performer must be taken in enough by their own performance so as to not seem fake in front of the audience. Performances are generally more convincing if the performer almost starts to believe in what

they are portraying as reality. An example can be found in video 10. After having spoken for a long time, gotten acquainted, and even sharing some personal beliefs with each other, the following exchange happened:

> Scambaiter: Tell, tell me about- tell me about yourself. What kind of- you know, you were saying we gotta eradicate all of the sin. What do you think is the best way to do that?
>
> Scammer: No hatred. No jealousy.
>
> Scambaiter: I guess that's what you're doing right now, huh? You're helping me.
>
> Scammer: No greed. Nothing should be there. Right? It should be pure. It should be pure help. (Video 10)

The scammer was speaking to the "victim" about how humans should help each other and not be greedy, which is rather ironic seeing how he was only pretending to help the "victim" to deceive him out of money. Although it is impossible to know for certain, a case can be made that he had convinced himself that the role he was playing was reality, and that he actually had a desire to help the victim simply for the sake of helping.

Even though they exhibited it in different ways, the vast majority of the scammers in the YouTube videos seemed to believe in their own performances to a fairly high degree. Although they spoke with various degrees of enthusiasm and alertness, the scammers appeared to have convinced themselves that they actually were professional technical support- or customer support workers to the degree that they kept up the performance when questioned or even directly confronted by the scambaiters. In video 2, the scambaiter admitted to the scammer that he is a scambaiter who at the time was live streaming their conversation. The following interaction then ensued:

> Scambaiter: So, what's- what's the company anyway that you can- everybody on the live stream can be aware of that's trying to scam people?

> Scammer: We're not scamming people.
>
> Scambaiter: Hang on. You've just done this live in front of 2000 plus people. So do you want to go back on that and try that again?
>
> Scammer: No, I'm not lying here. You had a problem with the computer, and you just contacted us. Right? (Video 10)

The scammer refused to acknowledge that the company he works for is actually a scam call center and maintained that they are simply helping people who are experiencing computer problems. After having been pushed further by the scambaiter, he became agitated:

> Yeah, but I thought like you are actually facing the problem because you told me that you are facing the problem. The computer is working slow, so that is for the lifetime support you are paying here. So if you don't have any problem, why you are paying then? (Video 10)

At that point, the scammer was likely upset that the scam, which he has invested two hours in, was not going to end successfully. However, he still seemed to be taken in by his own performance to the degree that it did not seem fake, and he displayed presence of mind by being able to answer to the allegations without breaking character. Maintaining his performance as a technical support worker who has been helping the "victim" with his issues, the scammer explained his anger by insinuating that the "victim" had wasted his time by acting interested in services he did not need. Although the scammer in this video maintained his performance until he eventually hung up the phone, some of the scammers in the videos ended up admitting that it was a scam after some pressure from the scambaiters. For example, the scammer in video 7 admitted rather quickly after it was made clear by the scambaiter that he knew that it was a scam:

> Scambaiter: All right, so do you like scamming people? Like why do you do it?
>
> Scammer: Just like that.

> […]
>
> Scambaiter: You're- you're robbing all these people blind. They don't even know that they're being robbed and you're robbing them. Stealing their money right in front of their faces. And you don't feel guilty about that at all?
>
> Scammer: No, it's not like that. See, you have a different perspective about it. (Video 10)

Although the scammer broke his performance and admitted that it was a scam, he refused to give comprehensive answers to the scambaiter's questions, and simply maintained that he had "a different perspective" (Video 10). Although it is impossible to know the scammer's actual thoughts and feelings, his answers can be interpreted as meaning that he felt no guilt, since he had his reasons for working at a scam call center which, in his mind, justified his fraudulent actions. Another plausible explanation for his behavior is that the scammer realized the immoral nature of his actions and did not know how to justify it. Hence, he chose to not even try, to avoid losing face by having to admit to fraud.

As mentioned, the scammers in the videos commonly used flattery as a manipulation tactic early in the phone calls. By the end of the conversations, however, the flattery was often exchanged with intimidation tactics and anger. For example, the scammer in video 6 who had previously complimented the "victim's" voice, was by the end of the conversation telling her that she needed to be smart, "because if you will be not smart, then you will face a lot of problems" (Video 6). Although this is a quite "soft" kind of intimidation compared to some of the scammers in the other videos, for example the social security scammer who threatened with arresting the "victim", it still aimed to instill her with the concern that if she made a mistake, she would face consequences. However, despite the fact that a majority of the scammers in the videos attempted to use intimidation tactics at some point, some changed strategies when realizing that the "victim" did not respond favorably to that intimidation. One such example can be found in video 5. After the "victim" started to redeem the gift cards on her own Google account, the scammer begun to angrily yell at her that it was his money, and that she was going to make him lose his job. This caused the "victim" to start crying and apologizing, which quickly changed the scammer's demeanor. Instead of yelling, he started to comfort the woman: "No, honey, I- I understand honey. Don't blame on yourself. It happens.

It happens. It happens." (Video 5). One possible reason for his sudden change could be that he is a disciplined performer who is able to use impression management to save the show, while it is also possible that he felt sympathy for the woman, as if he felt guilty for bringing her to tears.

After the scammers in the YouTube videos realized that they themselves had been "scammed" by the person they thought of as an unwitting victim, many of them responded with anger and expletive language. The scammer in video 10, for example, has the following response to realizing that he has been speaking with a scambaiter:

> Scammer: You're a moron. You know why? I'll tell you why you're a moron. You think yourself to be very smart.
>
> Scambaiter: You lost!
>
> Scammer: I, I didn't lost [sic] anything. You spoiled everything. (Video 10).

By refusing to acknowledge that he fell for the scambaiter's act and wasted his own time on trying to scam him, he instead called the scambaiter a "moron" and insinuated that he is not as smart as he thinks since his act was finally revealed. It could be understood as a desperate attempt to save face and stand victorious against the scambaiter by making him lose face instead. His final sentence, "you spoiled everything", can however be interpreted as him revealing how he truly feels about his scam being unsuccessful. Multiple scammers from the other videos also did not hesitate to let the scambaiters know how they felt about being tricked. Angry voices and phrases like "fuck off" (Video 3), "son of a bitch" (Video 9), and "you idiot" (Video 10) all occurred at the final stages of the conversations, right after the scambaiters' true motives had been revealed. Several of the online forum users also noted that scammers often get angry when they fail to achieve their desired outcomes. One user wrote the following in his post on the MSE forum under the thread "Phone scams": "I'll often string them along to the point where they hurl abuse at me and hang up." The scammers' performances are interrupted at these final stages, and for the first time, their true feelings make an appearance.

Scambaiters' performances and portrayal of victimhood

This chapter will focus on answering the second research question: How do scambaiters mislead scammers and perform victimhood through phone conversations? The scambaiters' performances in the YouTube videos will be described and analyzed using Goffman's (1956; 1967; 1974) theoretical framework. Christie's (1986) concept of the ideal victim will also be utilized to analyze how scambaiters attempt to portray themselves as believable victims in their conversations with scammers. The chapter will be divided into three parts, which discuss the beginning, middle, and end of the conversations depicted in the videos.

Beginning

Just as it is for the scammers, the introductory part of the phone conversations are of great importance to the scambaiters since it marks the start of their performances. How well they manage to create these performances will affect whether they manage to trick the scammers and make them believe that they are real potential victims or not. Although it is crucial for both scammers and scambaiters to convince the other of their respective performances, their goals differ in nature. While the scammers' main goal is monetary gain, the scambaiters work towards goals such as wasting scammers' time (Tuovinen & Röning, 2007), entertaining audiences (Sorell, 2019), and educating the public (Ross & Logi, 2021). The scambaiters' job is additionally to shame the scammers and make them lose face. However, achieving these goals might also cause monetary gain for the scambaiters, since they likely get paid when they post videos to YouTube.

All of the scambaiters in the videos were men, but several of them used voice changers in order to convincingly play the part of an old person, often a woman. Others, however, did not change their voice in any way. Once having called a number and being connected to a scammer, the scambaiters usually started their performances by introducing the problem that was the alleged reason for their call. After the scammer had introduced herself as "Jennifer" in video 1 and asked how she could help, the scambaiter answered the following: "Hi, Jennifer. I have a note on my email about an invoice from you guys. It says- but I- I don't know it, it says 'one BTC'?" (Video 1). By changing his voice to sound older and immediately establishing that he did not know what the invoice is regarding, or even what "BTC" was, the scambaiter attempted to portray himself as an ideal victim for the scammer.

As Christie (1986) argues, one factor which makes it easier for an individual to be perceived as a victim by society is weakness, which the scambaiter portrayed by playing the part of an old woman who does not possess a lot of knowledge on computers and technology. Although being unknowledgeable is not a factor which Christe (1986) uses as an example of weakness, it can be perceived as one in this situation, since knowledge in the area can usually prevent individuals from falling victim to technical support- or refund scams.

Just as it is favorable for scammers to create relationships with their victims, scambaiters can also benefit from these relationships. Whereas some scambaiters, similarly to some of the scammers, chose not to provide personal information during their conversations, others did. The scambaiter in video 2, for example, simply focused on the scam and did not share any personal information or try to establish a personal relationship with the scammer. In contrast, several other scambaiters continuously provided information about the character they were playing to encourage the scammer to do the same. An example can be found in the introductory part of one scambaiter's conversation with a scammer in video 6, where he played the role of an old woman:

> Scammer: Yeah, you have- so madam, because I'm still waiting. Okay? And I called you from the morning, from 10, yes, from 10 o'clock. Okay?
>
> Scambaiter: I know, I've- I've been sleeping all day. I'm very hung over. (Video 6)

It is common to react with amusement when confronted with events that challenge one's expectations (Sandberg & Tutenges, 2019, p. 565). The scambaiter's mentioning of being hung over could be interpreted as such a challenge, since it is not expected for an old lady to discuss her hangover with a customer support worker. This statement can hence be viewed as part of a comedic strategy that the scambaiter used to elicit amusement in his audience and ridicule the scammer. By instantly providing personal information about the lady he was portraying, the scambaiter further put an expectation on the scammer to act appropriately in response (Goffman, 1956). To act appropriately, in this case, would be for the scammer to convey that he was also comfortable with creating a personal relationship in which details about their private lives were shared. The scammer in this video did meet these expectations,

and instantly started displaying concern for the lady by saying that he had been thinking about her, and that he hoped that she was well. Although this scammer seemed to be open to adjust his performance to meet the presumed expectations of the scambaiter, not all scambaiters were as successful in creating this type of relationship with the scammers, although some tried. For example, the same scambaiter tried to share personal information with another scammer who did not seem willing to divert from his script:

> Scambaiter: My grandson helped me with all my passwords. I changed all of my passwords to the same password. That way it would be easier to remember.
>
> Scammer: Once you see your bank on your computer screen, please let me know. (Video 4).

While the scambaiter shared information about his character's grandson, the scammer did not even respond to this, and simply moved on with his script. This interaction can also be interpreted as the scambaiter displaying a weakness to cause the scammer to react, since individuals who possess knowledge about internet security know that it is not ideal to use the same password for multiple purposes. This weakness, combined with the fact that he was playing the role of an old person, makes his character a more ideal victim according to Christie's (1986) definition.

Though certain scambaiters might start off the conversations with performances that aim to establish a personal relationship and to portray themselves as ideal victims for the scammers, they also likely aim to achieve one of their main goals – to entertain their audience. As Tuovinen and Röning (2007) and Sorell (2019) argue, scambaiting can be a type of comedic art form, which uses a kind of humor that is not understood by the scammers but by only the scambaiters' Western audiences. Although the scambaiters in the videos commonly used more toned-down humor in the beginning of their conversations, probably to avoid suspicion from the scammers, they still introduced comedic aspects which set the tone for the rest of the conversations.

Once reaching the part of the conversations where the scammers had the opportunity to portray themselves as heroes capable of saving the victims from monetary loss, the

scambaiters in the videos usually responded appropriately and played the expected roles of victims. An example can be found in video 2:

> Scammer: What I can do with the virus, I can go ahead and remove all those virus [sic].
>
> Scambaiter: Okay.
>
> Scammer: And repair all the damages, clean up your entire network, okay? So that you can use internet and computers and there will be no problem. Alright?
>
> Scambaiter: Right. Good, thank you. (Video 2)

While the scammer established his role as the hero who can help the victim, the scambaiter simply played along and pretended like he was an unknowing victim who was grateful for the help he was getting. Although most of the scambaiters in the videos played along in a similar manner, not everyone did. The scambaiter in video 10, for example, refused to play the expected role of the grateful victim. After the scammer had introduced himself as "Alex Ross from PayPal" (Video 10), the scambaiter angrily asked why a payment had been authorized without his approval:

> Scammer: Tell me, this is Alex Ross from PayPal. How may I help you today?
>
> Scambaiter: Well, I don't know if you can help me unless you can- you can explain to me why you authorized a payment for $659 without my permission. If you can explain that to me, then maybe you can, Alex. (Video 10)

In this video, the scambaiter challenged the scammer by not adhering to the societal norms which according to Goffman (1956) usually cause individuals to treat others appropriately in

relation to how they act. The scammer attempted to play the hero, but was interrupted before his performance could even properly begin.

As previously discussed, the scammers in the videos commonly used flattery as a manipulation tactic in the early stages of the conversations. In the instances when this occurred, the scambaiters more often than not played along and pretended to be flattered. Aside from adding entertainment value, the scambaiters' response to being complimented can be interpreted as a method they use to make the scammers believe that their manipulation tactic is effective, so that they are more likely to proceed with the scam. It also helps them create performances as naïve victims who believe everything the scammers tell them. In video 6, after the scammer told the "victim" that she had a nice voice, the scambaiter answered the following: "Oh, thank you. I've never had somebody be so nice to me" (Video 6). The scambaiter responded according to what he interprets to be appropriate, in order to make the scammer feel satisfied and certain that the "victim" is buying his act. Once the scammer is convinced of this, it gets easier for the scambaiter to successfully scam the scammer back.

Scamming the scammer and ideal victimhood

After having introduced the roles they are playing and laying the foundation for the entertainment aspects, the scambaiters enter the second part of their conversations with scammers. When asked by the scammers to download a remote access program on their computers, the scambaiters usually continued to play along as unwitting victims who did not understand what it was or why they were asked to download it, but nevertheless complied. An example can be found in video 1, when the scammer requested the scambaiter to open Google Chrome so that she could further give him instructions on how to download a remote access program:

> Scammer: Okay. Just go ahead and open your Google Chrome, okay? And once you open your Google Chrome, do let me know. I'll guide you further from there.
>
> Scambaiter: Okay. I'm sorry. I'm not the best on this thing. Um, okay. (Video 1)

Again pointing to the fact that his character does not possess a lot of knowledge on computers, the scambaiter attempted to convince the scammer that he was the person he was portraying. One of the main goals of scambaiting is to waste scammers' time and resources and to get revenge on behalf of actual victims (Tuovinen & Röning, 2007), which is why it is favorable for them to maintain the fabrication that they are actual potential victims for as long as possible. As the conversations progressed, the scambaiters in the videos who focused on comedic value began to add more and more entertainment features. In some cases, having established a successful personal relationship with the scammer proved beneficial, since the scammers in these cases were more likely to participate in the comedic interactions. An example of this can be found in video 9, after the scambaiter has played a song for the scammer which he claimed was his character's late husband's. While the scammer made an attempt to proceed with the scam, the scambaiter played the song again, and asked the scammer the following: "Oh do you want to sing along? I would love that so much." (Video 9). Having succeeded in establishing the basis for a personal relationship, the scammer complied with the request and quietly started singing along to the song. Probably content that he managed to produce valuable comedic material, the scambaiter smiled at the camera.

While the scambaiters were obviously having a conversation with the scammers, they simultaneously had another conversation with their audience. In the live streamed videos, these conversations were direct, since the scambaiters could communicate with their audience in real time while scamming the scammers. The audience could hence participate in the conversations by commenting and making suggestions (Ross & Logi, 2021). An example can be found in video 2, where the scambaiter hosting the livestream incorporated a suggestion from a commenter and pretended that he had a dog in the background who was misbehaving and who he constantly had to yell at. In the edited YouTube videos, the scambaiters communicated with the audience through explanations about what was happening in the scam, facial expressions, and other mannerisms. Although the audience could not respond in real time, they could offer their opinions and thoughts through the comment section. An additional mode of communication is the humor that is utilized by the scambaiters. As previously mentioned, is has been argued by Sorell (2019) that scambaiters use inside jokes that the audience understands and finds entertaining, while the scammers are unaware of the humor. A theme which can be found in several of the videos, is that the scambaiters referred to common words or phrases which are often used by scammers. Two examples that are mentioned in several videos are the phrase "each and everything" and the word "dextop", a

mispronunciation of the word “desktop”. For example, the scambaiter in video 6 repeated the phrase “each and every day” when it was mentioned by the scammer:

> Scammer: No, I'm just- because yesterday I told you, madam, that tomorrow I will talk with you entire day. I hope you remember right? Because you are alone. So that's a reason. Okay? […] Not only for today, okay? Each and every day I will give my entire day, okay?
>
> Scambaiter: Each and every day? (Video 6)

The utilization of these words and phrases function as a type of superiority comedy which aims to belittle the scammers and make the scambaiters feel triumphant in comparison (Sandberg & Tutenges, 2019, pp. 565-566). While the scammers in the videos did not seem to realize that they were being ridiculed, the scambaiters and their audiences understand the comedic value that the mentioning of these words and phrases holds. Since the audiences know that the scambaiters are putting on a show, they possess information that the scammers do not. The reality which is portrayed to the scammers, on the other hand, is the fabrication that the scambaiters have created in order to scam them back. This is facilitated by the factors which Goffman (1974, pp. 449-450) mention, one of these being that the scammers could only act upon the information available to them: the information conveyed by the scambaiters. The scambaiters in the videos also commonly edited the information displayed on their computer, for example the wallpaper, the photos, and the name, to match the characters who they were portraying.

Apart from introducing more entertainment aspects, the scambaiters continued to develop their characters’ personalities in the second part of the phone conversations. In the videos in which the scambaiters portrayed old people, they often depicted these as naïve and grateful for the help they were getting. An example can be found in video 5, when the scambaiter told the scammer the following:

> Thank you so much. Finally. It is nice talking to you. I really appreciate your time and your patience. I know it's not easy working

> with someone my age and you really went above and beyond in terms of just being patient and waiting for me […] (Video 5)

Acting grateful towards the scammer and referring to "her" own old age could presumably serve a few different purposes for the scambaiter, the first being to appeal to the scammer's conscience and making him feel guilty for scamming an old and naïve woman who was under the impression that he had helped her. A second purpose could potentially be to further portray his character as an ideal victim, the age and naiveness serving as weakness factors. In some of the videos, the scambaiters seemingly attempted to portray themselves as weak, whereas the scammers were portrayed as powerful in comparison. In video 8, the scambaiter acted scared when the scammer told him that he is a "federal officer": "But you are scaring me, right? You're telling me about all these charges and all these things that can happen to me. Like that's not- oh my goodness. Like I'm so scared right now. Right?" (Video 8). By drawing attention to the scammer being in a position of power, he is portrayed as the "big and bad" offender which Christie (1986) argues is necessary in order for a victim to be viewed as ideal.

Although the characters who the scambaiters portrayed in the videos possessed certain characteristics which according to Christie (1986) makes someone an ideal victim, they failed to achieve all of the necessary requirements. According to Christie (ibid.), ideal victims are in a place they cannot be blamed for being at. This requirement is impossible for fraud victims to fulfill, since they as Cross (2018) argues, are considered contributors to their own victimization. Among the scam descriptions on online forums, many posters also seemed to be of the opinion that victims of scams largely have themselves to blame for their victimization. One user posted the following to the Reddit forum r/AskReddit under the thread "What's your funniest scam call story?", when describing one victim's story:

> She cleared out her whole bank account to buy the gift cards, when the total amount she withdrew would have been more than enough to buy a new computer. The situation itself wasn't actually fun. But the blatant stupidity of this woman is actually quite funny. (Reddit, r/AskReddit)

The poster calls the victim stupid for having fallen for the scam, alluding that she is partly to blame for her own victimization. Other online forum posters seemed to share this opinion, as they frequently called themselves stupid for having fallen for a scam or came up with explanations to justify their own or their family member's "stupidity". Building on the supposition that scam victims are commonly viewed as rather unintelligent, the scambaiters' portrayal of their characters as naïve and uninformed could be interpreted as them sharing this stereotypical view, and therefore conveying their characters accordingly. Like the young shoplifters in Katz's (1988) work imitated the behaviors of normal customers, the scambaiters in the videos attempted to mimic the characteristics of their idea of a typical scam victim.

Resolution

As mentioned in the previous chapter, the final part of the conversations largely consisted of the scambaiters testing the scammers and pushing them to their limits. Apart from starting to question their true motives, the entertainment factor reached its peak in the final stages in multiple of the YouTube videos. After having been asked by the scammers to drive to the nearest convenience store and purchase gift cards in the refund scams, several of the scambaiters pretended to drive to a store, buy gift cards, and drive back home again, while the scammers stayed on the line. The scambaiter in video 10 explained to his audience why this part is of great importance:

> So, this part's sort of- this is a crucial moment in his script. The second I get in that car, he's gonna ask me to scratch off the codes and give it to him. I don't want to do that. I want to redeem these cards. So, I have to make up a reason. (Video 10)

The scambaiter then proceeded to log into his computer, and while the scammer asked him to give him the code on the back of the card, the scambaiter claimed that he needed to figure out what to do with it on the computer first. The scammer could be heard protesting loudly on the phone as the scambaiter started typing the gift card codes into his Google Play account and redeeming them himself. According to Sorell's (2019) findings, scambaiters aim to deceive scammers by slowly making them realize that they have been tricked, and hence making them

increasingly angry. After maintaining the scammers hopeful of a successful scam for the entirety of their conversations, the scammers' eventual rage served as an important comedic aspect for the scambaiters and their audiences. It was seemingly no longer as important for the scambaiters to convincingly play the parts of victims as it was to create a big, comedic ending which would entertain their audiences. They also seemed to find amusement in seeing how far they could go with annoying the scammers before they had had enough.

Although some of the scammers in the videos ended the conversations quickly after realizing that they would likely not receive any money, others patiently continued to speak with the scambaiters. A few of the scambaiters further used what Goffman (1956) calls impression management to attempt to maintain the conversations. Behaviors which can be interpreted as displays of dramaturgical loyalty and dramaturgical discipline (ibid.) were displayed by several scambaiters. An example can be found in video 5. While the scambaiter started redeeming the gift cards to his own account, the scammer furiously screamed for him to stop. However, once they had been redeemed, the scambaiter apologized for the "mistake" while pretending to cry: "I'm sorry. I wish it could have been different. I feel so bad!" (Video 5). The scambaiter stayed loyal to his performance as an old, naïve lady who lacked knowledge when it comes to modern technology, and therefore made a mistake. He also displayed presence of mind by pretending to feel guilty about the mistake, and even proved this by crying. This can also be interpreted as a display of emotion work, which Hochschild (1979) describes as the act of attempting to evoke, shape, or suppress an emotion to portray oneself in a specific way. In this case, the scambaiter evoked feelings of sadness and guilt to portray himself as a well-meaning old woman who simply made an honest mistake. Furthermore, he played the role convincingly enough so that he seemed taken in by his own performance.

As aforementioned, the final parts of the conversations in the videos were commonly used by the scambaiters to question the scammers' motives, and sometimes even directly confronting them. Whereas the scambaiters sometimes started asking questions at various points in the conversations, they waited to confront them and reveal their true intentions until the very end. One reason for this might be that they wanted to distract the scammers for as long as possible, but once they realized that they were unable to keep speaking to the scammers unless they actually sent them money, they opted for a big, satisfying ending instead. An example of a scambaiter who eventually did admit to the scammer that he was not an actual victim can be found in video 2, in which the scambaiter started off by questioning the scammer on where he is from, and then revealed that he is a scambaiter: "You're about to be famous on YouTube.

Do you know that?" (Video 2). While the scammer continuously denied being a scammer, the scambaiter proceeded to tell him about his YouTube channel and even how to find it. At that point, the scambaiter had completely abandoned his previous performance, and was presumably focusing solely on creating a satisfactory ending for both his viewers and for himself while shaming the scammer.

In a few of the videos, the scammers realized that they were being tricked before the scambaiters had the chance to willingly admit it. This was the case in video 1:

> Scammer: Are you the hacker? Hello?
>
> Scambaiter: I'm sorry?
>
> Scammer: Uh, you are the hacker.
>
> Scambaiter: What does that mean?
>
> Scammer: You're trying to hack me. (Video 1).

When being accused by the scammer of being a "hacker", the scambaiter initially attempted to use impression management and save face by pretending to be clueless about what the scammer was referring to. Although the scammer continued with his script for a few more minutes, he ultimately decided to hang up. The scambaiter's attempt at impression management hence proved unsuccessful.

Although the majority of the scambaiters decided to stop playing the part of victims once the scammer realized their true motives, or the scambaiters themselves admitted their acts, the scambaiter in video 10 proceeded with his performance even after the scammer seemingly realized that the "victim" had willingly wasted his time:

> Scambaiter: You, oh, you snake. I get it now. I get it. That's why you're mad. You're saying I wasted your time. You don't get paid for this, do you? This isn't your job. You were trying- and that's why you didn't want me to tell the lady at the store. That's why-

Scammer: You're wasting time. You know you're wasting time.

Scambaiter: Oh my God. (Video 10).

While still portraying a victim who had fallen for the scam up until this point, the scambaiter pretended to have just realized that it had all been an attempted fraud. As the conversation progressed, and the scammer seemed upset about having been tricked, the scambaiter told the scammer the following: “At least- at least I don't prey on innocent old men and try to steal their money. You couldn't steal them. You couldn't steal from a- did you realize that you couldn't even steal from a 70-year-old?” (Video 10). The scambaiter seemingly attempted to make the scammer feel guilty for trying to steal money from an old man, while simultaneously making fun of him and causing him to lose face for not being able to successfully do so. It might also be interpreted as the scambaiter being aware of the fact that he has also committed a morally “wrong” act by deceiving the scammer, but he instead chooses to focus on the scammer’s wrongdoing. After continuing with the conversation in a similar manner for a few additional minutes, the scammer told the scambaiter “I am done talking to you” (Video 10) and hung up the call. The scambaiter, just like most of the scambaiters in the videos, had successfully achieved the goals mentioned by Tuovinen and Röning (2007) and Sorell (2019): he had played the role of a victim and hence wasted the scammer’s time and resources while simultaneously entertaining and educating his audience.

Concluding discussion

The purpose of this thesis has been to investigate which techniques both scammers and scambaiters use in order to trick and manipulate the other through verbal communication via phone calls. Goffman's (1956; 1967; 1974) theoretical framework has been applied throughout the analysis to gain an understanding of the performances that scammers and scambaiters use in their phone conversations to credibly portray characters which they consider beneficial to achieve their desired goals. The scammers in the YouTube videos mainly portrayed themselves as professional and competent customer support- or technical support workers, frequently playing the part of the "hero" capable of saving their "victims" from monetary loss. They further attempted to create trusting relationships with the "victims" in order to instill them with a false sense of security and make them more willing to ultimately send money to the scammers. While the majority of the scammers utilized impression control and displayed dramaturgical discipline by adjusting their narratives to appropriately respond to specific "victims", they frequently used manipulation techniques such as flattery early in the conversations, and intimidation at the later stages. In the refund scams, the scammers regularly introduced a shift in the narrative in the middle of the conversations, claiming that a mistake had been made and that it was now the "victims'" responsibility to play the role of the hero who could save the scammers from loss of employment. Techniques such as pleading to the victims' conscience were frequently utilized by the scammers to get the "victims" to comply.

The scambaiters in the YouTube videos typically played the roles of characters they presumably considered to be ideal victims for the scammers: old, naïve, and non-technical women or men. Although fraud victims fail to qualify as ideal victims according to Christie's (1986) definition, since they are considered contributors of their own victimization (Cross, 2018), the scambaiters in the videos included attributes in their performances such as weakness and powerlessness in relation to the scammers, which can be interpreted as an attempt to portray themselves as more ideal victims. Although some of the scambaiters did not play roles which were distinctly different from their own selves, and instead seemingly focused on authentic, educational conversations with the scammers, others made an effort to put on over-the-top performances with the likely purpose of entertaining their audience and making the scammers lose face. To achieve the entertainment aspect, they used the comedic art form discussed by Sorell (2019), which consists of a type of humor understood by the

scambaiters' Western followers but not by the scammers, and which aims to gradually make the scammers realize that they have been deceived, resulting in increasing anger. This humor further serves to ridicule and belittle the scammers, as well as functioning as a form of revenge. The scammers, who are usually the perpetrators, are instead turned into victims of ridicule.

Another conclusion that can be drawn from the analysis is that the behaviors and techniques of the scammers and the scambaiters in the videos affect each other. Both parties portray themselves in certain ways hoping that the other will respond appropriately, and they adjust their behaviors depending on their assessment of what will lead to the most favorable outcome. In the cases where the scambaiters portrayed themselves as old, naïve men or women who provided the scammers with plenty of personal information, the scammers usually responded by using this personal connection to make the "victims" feel safe and content. However, when the scambaiters kept their performances closer to their actual selves and did not share any personal information, the scammers typically maintained a professional relationship and simply focused on the issue the "victims" were allegedly experiencing. Likewise, the scambaiters acted upon the scammers' performances. If, for example, they received a compliment from a scammer, the majority of the scambaiters saw this as a chance to continue displaying affection and see how far they would go. When the scambaiter in video 6 received a compliment on his voice, he used this as an opening to continue using affectionate language. At one point he even went as far as to tell the scammer "I love you" (Video 6), and triumphantly smiled at the camera when the scammer said it back.

An aspect worth noting is that although the scammers are portrayed as the offenders while the scambaiters perform the roles of victims during their conversations, this dynamic is not indisputable. One can argue that scammers' motives for tricking their "victims" is more sinister since they aim to defraud them out of money, but nevertheless, the scammers can also be viewed as victims of the scambaiters' deception. The scambaiters exploit the scammers in order to achieve their goals. Apart from wasting their time, producing entertainment, and educating their audiences, some of the scambaiters in the videos even attempted to gain access to the scammers' computers to obtain information that could be handed over to authorities. In other words, the scammers and the scambaiters both lie and manipulate while trying to scam each other and reach their respective goals.

As mentioned in the introductory part of this thesis, there is a lack of research concerning scams, scammers, and scambaiting, as the majority of the research conducted on this area has mainly focused on victims' accounts and the objectives of scambaiting as well as how scambaiting is conducted on online platforms, and whether it is ethical or not. This thesis has utilized recorded conversations between scammers and scambaiters to firstly gain an understanding of how scammers verbally manipulate their potential victims through phone conversations, and secondly, how scambaiters mislead scammers and perform victimhood through phone conversations. Seeing the different types of scams being conducted and how the number of people losing money to scams increases every year, future research is needed to produce further knowledge on this subject, which can help prevent scams. One way to produce such knowledge would be to continue to gain an understanding of how scams play out by identifying typical scenarios and raising awareness among the public. Another way would be to gain an understanding of the reasons scammers choose to conduct scams. By recognizing the scammers' own perspectives and how they morally justify their actions, one might be able to gain knowledge which can be used to discourage individuals from turning to fraud.

Research on scambaiting can additionally highlight important aspects of contemporary cultures of online shaming, and how these are communicated through online forums. With the constant development of the Internet and social networking sites, scambaiting and other forms of online vigilantism and online shaming is more easily conducted and spread to large audiences. Researching how and why these individuals choose to participate in these activities could offer valuable insights into this deceptive behavior and its consequences. It further serves as an interesting starting point for a discussion on when deception is considered acceptable, and when it is not.

References

America's Cyber Defence Agency (n.d.). *Common Scams*. Available at: https://www.cisa.gov/be-cyber-smart/common-scams [Accessed 28 Feb. 2023].

Anderson, R. (2007). *Thematic Content Analysis (TCA)*. Available at: https://rosemarieanderson.com/wp-content/uploads/2014/08/ThematicContentAnalysis.pdf

Bakar, S. N. A. & Zakaria, N. H. (2021). "The Impact of Fear and Rational Appeal Scam Techniques on Individual Susceptibility", *Baghdad Science Journal, 18*(2), 871-883. https://doi.org/10.21123/bsj.2021.18.2(Suppl.).0871

Bosma, A., Mulder, E. & Pemberton, A. (2018). "The ideal victim through other(s') eyes", in Duggan, M. (ed.) *Revisitig the 'Ideal Victim'*. Bristol: Bristol University Press.

Braun, V. & Clarke, V. (2006). "Using thematic analysis in psychology", *Qualitative Research in Psychology, 3*(2), 77-101.

Butler, J. (2008). *Sexual Politics, Social Change and the Power of the Performative*. London: Routledge.

Button, M. & Cross, C. (2017). *Cyber Frauds, Scams and their Victims*. New York: Routledge.

Cassiman, A. (2019). "Spiders on the World Wide Web: cyber trickery and gender fraud among youth in an Accra *zongo*", *Social Anthropology, 27*(3), 486-500. https://doi.org/10.1111/1469-8676.12678

Christie, N. (1986). "The Ideal Victim", in Fattah, E. A. (ed.) *From Crime Policy to Victim Policy*. London: Macmillan.

Collins English Dictionary (n.d.). Available at: https://www.collinsdictionary.com/dictionary/english/scambaiting [Accessed 13 April 2023].

Cross, C. (2018). "Denying victim status to online fraud victims: the challenges of being a 'non-ideal victim'" in Duggan, M. (ed.) *Revisitig the 'Ideal Victim'*. Bristol: Bristol University Press.

Deck, A. & Kumar, R. (2023). “Vigilantes for views: The YouTube pranksters harassing suspected scam callers in India”, *Rest of World*, 10th January. https://restofworld.org/2023/youtube-scam-call-vigilantes/

Dynel, M. & Ross, A. S. (2021). “You Don’t Fool Me: On Scams, Scambaiting, Deception, and Epistemological Ambiguity at R/scambait on Reddit”, *Social Media + Society*, 1-14. https://doi.org/10.1177/20563051211035698

Ellis, P. (2020). “Sampling in qualitative research 1”, *Wounds UK, 16*(3), 82-83.

Etikan, I., Musa, S. A. & Alkassim, R. S. (2016). “Comparison of Convenience Sampling and Purposive Sampling”, *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4. https://doi.org/10.11648/j.ajtas.20160501.11

Federal Trade Commission (2022). *Who experiences scams? A story for all ages*. Available at: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages [Accessed 7 March 2023].

Fraud.com (n.d.). *The History and Evolution of Fraud*. Available at: https://www.fraud.com/post/the-history-and-evolution-of-fraud [Accessed 1 March. 2023].

Goffman, E. (1956). *The Presentation of Self in Everyday Life*. London: Penguin Books.

Goffman, E. (1967). *Interaction Ritual: Essays on Face-to-Face Behavior.* New York: Pantheon Books.

Goffman, E. (1974). *Frame Analysis: An Essay on the Organization of Experience*. Boston: Northeastern University Press.

Hochschild, A. R. (1979). “Emotion Work, Feeling Rules, and Social Structure”, *American Journal of Sociology, 85*(3), 551-571.

Johansson, A. (2005). *Narrativ teori och metod*. Lund: Studentlitteratur.

Jung, C. G. (1967). *Two Essays on Analytical Psychology*, Collected Works of C. G. Jung, Volume 7. Princeton: Princeton University Press.

Katz, J. (1988). *Seductions of Crime: Moral and Sensual Attractions in Doing Evil*. New York: Basic Books.

Kazlauskas, J. (2023). “Teen loses $25,000 after falling for phone scam”, *New York Post*, 7th January. https://nypost.com/2023/01/07/teen-loses-25000-after-falling-for-phone-scam/

Lester, D., Tzani-Pepelasi, C., Gavrilovic Nilsson, M., Roumpini Pylarinou, N. & Ioannou, M. (2020). “Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics”, *Journal of Forensic and Investigative Accounting*, *12*(1), 163-178.

http://web.nacva.com/JFIA/Issues/JFIA-2020-No1-10.pdf

Levi, M. (2008a). “Organized fraud and organizing frauds: Unpacking research on networks and organization”, *Criminology & Criminal Justice, 8*(4), 389-419. https://doi.org/10.1177/1748895808096470

McCart, C. (2022). “35+ Phone Spam Statistics for 2017 – 2022”, *Comparitech*, 29th July. https://www.comparitech.com/blog/information-security/phone-spam-statistics/

Mead, G. H. (1913). “The Social Self”, *The Journal of Philosophy, Psychology and Scientific Methods, 10*(14), 374-380.

Morgan-Bentley, P. & Good, A. (2019). “Action Fraud investigation: victims misled and mocked as police fail to investigate”, *The Times*, 15th Aug. https://www.thetimes.co.uk/article/action-fraud-investigation-victims-misled-and-mocked-as-police-fail-to-investigate-wlh8c6rs6

Mujezinovic, D. (2022). “What is Scambaiting? Here’s Everything You Need to Know”, *Make Use Of*, 13 December. Available at: https://www.makeuseof.com/what-is-scambaiting/

Muncaster, P. (2023). *Tech support scammers are still at it: Here’s what to look out for in 2023*. Available at: https://www.welivesecurity.com/2023/01/19/tech-support-scammers-still-at-it-what-look-out-for/ [Accessed 1 March 2023].

NT.GOV.AU (2015). *Ten most common types of scams.* Available at: https://nt.gov.au/law/crime/scams/ten-most-common-types-of-scams [Accessed 28 Feb. 2023].

Riessman, C. K. (2005). “Narrative Analysis”, in Kelly, N., Horrocks, C., Milnes, K., Roberts, B. & Robinson, D. (eds.) *Narrative, Memory & Everyday Life*. Huddersfield: University of Huddersfield.

Rock, P. (1986). “Society’s Attitude to the Victim”, in Fattah, E. A. (ed.) *From Crime Policy to Victim Policy*. London: Macmillan.

Ross, A. S. & Logi, L. (2021). “’Hello, this is Martha’: Interaction dynamics of live scambaiting on Twitch”, *Convergence: The International Journal of Research into New Media Technologies, 27*(6), 1789-1810. https://doi.org/10.1177/13548565211015453

Sandberg, S. & Tutenges, S. (2019). “Laughter in stories of crime and tragedy: The importance of humor for marginalized populations”, *Social Problems, 66*(4), 564-579. https://doi.org/10.1093/socpro/spy019

Schaffer, D. (2012). “The Language of Scam Spams: Linguistic Features of “Nigerian Fraud” E-Mails”, *ETC: A Review of General Semantics, 69*(2), 157-179. https://www.jstor.org/stable/42579182

Schultz, B. (2022). “Millions of Americans lose money to scams every year. One group of YouTubers is trying to help.”, *USA Today*, 13th October.

Shaari, A. H., Kamaluddin, M. R., Fauzi, W. F. P. & Mohd, M. (2019). “Online-Dating Romance Scam in Malaysia: An Analysis of Online Conversations Between Scammers and Victims”, *Journal of Language Studies, 19*(1), 97-115. http://doi.org/10.17576/gema-2019-1901-06

Smallridge, J., Wagner, P. & Crowl, J. N. (2016). “Understanding Cyber-Vigilantism: A Conceptual Framework”, *Journal of Theoretical & Philosophical Criminology,* 8, 57-70.

Sorell, T. (2019). “Scambaiting on the Spectrum of Digilantism”, *Criminal Justice Ethics, 38*(3), 153-175. https://doi.org/10.1080/0731129X.2019.1681132

Tait, A. (2021). “Who scams the scammers? Meet the scambaiters”, The Guardian, 3rd October. https://www.theguardian.com/technology/2021/oct/03/who-scams-the-scammers-meet-the-amateur-scambaiters-taking-on-the-crooks

Truecaller (2022). “Truecaller Insights 2022 U.S. Spam & Scam Report”, *Truecaller*, 24th May. https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report

Tuovinen, L. & Röning, J. (2007). “Baits and beatings: Vigilante justice in virtual communities”, *Proceedings of CEPE 2007: The 7th International Conference of Computer Ethics: Philosophical Enquiry*, 397-405.

USA gov. (2022). *Common Scams and Frauds.* Available at: https://www.usa.gov/common-scams-frauds [Accessed 28 Feb. 2023].

Whittaker, J. M. & Button, M. (2021). "'Scambaiting': why the vigilantes fighting online fraudsters may do more harm than good", *The Conversation*, 21st June.

Whitty, M. T. (2013). "The Scammers Persuasive Techniques Model: Development of a stage model to explain the online dating romance scam", *British Journal of Criminology, 53*(4), 665-684. https://www.cl.cam.ac.uk/~rja14/shb17/whitty.pdf

419Eater (n.d.). *419Eater: scambaiting community.* Available at: https://aff.419eater.com/. [Accessed 8 March 2023].

Wiles, R. (2013). *What are qualitative research ethics?* London: Bloomsbury.