Application of crowdsourcing platforms for fighting telephone scams

Academic paper to obtain the degree of

Bachelor of Arts

in the study program

Economic Studies

Abstract

Telephone scams and spam calls are a widespread problem, especially across English-speaking countries. Call centers, usually based in India, try to defraud people using scare tactics, impersonation, and other techniques. Online vigilantes, so-called “scambaiters”, try to fight these scammers. They gather in communities and use specific tools and methods which can be characterized as crowdsourcing. This thesis uses one such tool, BobRTC, as a case study to analyze if and how these methods can contribute to influence or obstruct the activities of the telephone scammers and if the scammers feel an impact on their work due to scambaiting activities. For this reason five scambaiters and four scammers have been interviewed. As result it can be concluded that crowdsourcing methods can have a significant impact on the scam call centers, depending on the methods used and the concentration of users on one particular call center.

Content

Abstract II
Content III
Figures IV
Tables V
Abbreviations VI
1 Introduction 1
1.1 Background and motivation 1
1.2 Structure of the thesis 4
2 Theoretical background and terms 6
3 Method 15
3.1 General method 15
3.2 Case 15
3.3 Data collection 19
3.4 Data analysis 22
4 Findings 25
5 Discussion 31
6 Conclusion 34
6.1 Limitations 34
6.2 Future research topics 36
6.3 Summary 37
References VII
Appendix XIV
Declaration of Academic Integrity XVIII

Figures

Figure 2-1: Caller ID spoofing 6
Figure 2-2: Fake pop-up message 9
Figure 3-1: BobRTC phonebook 17
Figure 3-2: BobRTC dial page 17
Figure 3-3: Process model of structuring content analysis 23
Figure 4-1: Word cloud scambaiter interviews 29
Figure 4-2: Word cloud scammer interviews 30

Tables

Table 3-1: List of interviewees 21

Abbreviations

US	United States
FCC	Federal Communications Commission
FTC	Federal Trade Commission
FBI	Federal Bureau of Investigation
ICO	Information Commissioner’s Office
Ofcom	Office of Communications
IRS	Internal Revenue Service
SSA	Social Security Administration
VoIP	Voice-over-IP
STIR	Secure Telephone Identity Revisited
SHAKEN	Signature-based Handling of Asserted Information Using toKENs
CBI	Central Bureau of Investigation
SEA	Search Engine Advertising
VPN	Virtual Private Network

1 Introduction

1.1 Background and motivation

“This call is regarding to your Social Security Number. We found some fraudulent activities under your name. Please call us back immediately in order to resolve this issue.”

First Orion, a telecommunication solution provider, estimated in 2018 that half of all calls to mobile phones throughout the US in 2019 will be robocalls, similar to the one above, a drastic increase from previous years (First Orion, 2018, p. 1). This telecommunication solution provider filters and blocks unwanted spam/robocalls from consumer devices (First Orion, 2018, p. 1). It turned out to be “just” 40% for 2019 (First Orion, 2019, p. 2). However, that is still a considerable number Robocalls are automated, computer-generated calls, which can be scam or spam calls. Scam calls are also called fraudulent calls; their aim is to steal the call recipient’s money, or personal information and are thus illegal. Spam calls, on the other hand, are unwanted or unsolicited calls to make sales, often done by telemarketers or robocallers. They are illegal without prior consent. The Federal Communications Commission (FCC), which supervises telecommunications-related issues in the United States, reports that around 232,000 complaints were received in 2018 about unwanted phone calls, an increase to the figures of 2015 of 172,000 (Federal Communications Commission, 2019, p. 4). The Federal Trade Commission (FTC) reports 3.6 million complaints for 2015 and 5.8 million in 2018, a huge increase in only 3 years (Federal Communications Commission, 2019, p. 5). The FTC also states that their National “Do Not Call” Registry, which companies have to check before making telemarketing calls, has grown to 239.5 million actively registered phone numbers in 2019 (FTC, 2019, p. 1). With a population of 328.2 million in 2019 in the United States, that would mean around 73% of the population do not wish to receive telemarketing calls and felt urged to put their number on that list, given we assume one telephone number per person (US Census Bureau, 2019, p. 1). YouMail, a technology provider for call filtering and blocking, estimates that the national volume on robocalls amounted to around 48 billion calls in 2018 and, for example, they show that in November 2018 there were about 2,000 calls per second (Federal Communications Commission, 2019, p. 6). Tech support scams are part of fraudulent

calls. A study by Microsoft's Digital Crimes Unit has shown that three out of five consumers have been exposed to tech support scams in 2018 (Microsoft Digital Crimes Unit, 2018). The Federal Bureau of Investigation (FBI) reports in its annual Internet Crime Report of 2019 that they received over 13,000 complaints regarding tech support scam alone, from victims in 48 countries and $54 million in damages, which is a 40% increase to 2018 (Federal Bureau of Investigation, 2019, p. 13). These days, scammers use the COVID-19 pandemic to exploit the people's anxiety and are blasting themed robocalls across the nation (FTC, 2020, p. 1).

In the United Kingdom, the Information Commissioner's Office (ICO) and the Office of Communications (Ofcom) reported 124,363 complaints in 2018 and, their studies have shown that still 49% of all adults in the UK who own a landline, a mobile phone or both have been targeted by nuisance calls (which include live and recorded marketing calls, silent calls, and abandoned calls) in 2019 (Ofcom, 2019, p. 3). While the number of complaints to ICO and Ofcom seems to be relatively constant for the third year in a row, it still shows it is a massive problem, and we are only at the beginning to tackle it, reversing a decade long trend of increasing complaints (Ofcom, 2019, p. 2).

Fighting phone fraud is a complicated undertaking: The United Kingdom's ICO reported in a meeting of Operation LINDEN, a group of stakeholders such as regulators, consumer groups, and industry representatives, in February 2020 that out of 37 investigations for unsolicited marketing calls and texts over the last 12 months, 30 had to be closed due to companies liquidating, a lack of evidence presented or the perpetrators being located outside of the country and thus outside of the jurisdiction (Clancy et al., 2020, p. 2; Ofcom, 2019, p. 8; Tzani-Pepelasi, Nilsson, Lester, Pylarinou, & Ioannou, 2020, p. 165). Only six monetary penalties have been issued with fines totaling £700,000 (Clancy et al., 2020, p. 2). The Data & Marketing Association which is part of Operation LINDEN reports increased scam calls over the previous years (Clancy et al., 2020, p. 5). That shows that the ICO's initiated investigations are not enough to combat fraudulent calls efficiently. Meanwhile, in the United States, the FTC and FCC sent joint letters to multiple Voice-over-IP (VoIP) carriers warning them of transmitting Covid-19 related scam calls could result in law enforcement actions against them and even did so in two other cases in January 2020 so recently, there is some urgency however that usually

is not often the case (FTC, 2020; US Department of Justice, 2020b, 2020c). Law enforcement and police of victimized countries are also trying to fight, but they have to rely on collaboration with the local Indian police, the country where a huge part of the scam call centers are located (Microsoft Digital Crimes Unit, 2018, p. 5; Miramirkhani, Starov, & Nikiforakis, 2017, p. 12). This happened in September 2020 when, for the first time in history, the Indian Central Bureau of Investigation (CBI) collaborated with the US authorities for a sting operation against one of the biggest tech support fraud call centers with raids against several other companies based in India but also against individuals and companies in the US (US Department of Justice, 2020a). Also, Germany's public prosecutor's office in Osnabrück, in conjunction with the LKA Niedersachsen, raided a call center based in Kolkata together with Indian police in May 2016 to probe the reports of duped Germans (Staatsanwaltschaft Osnabrück, 2016).

However, these few call center busts are not enough to fight call center fraud as they are not enough to deter scammers from running their business as it can be seen that the numbers of scam and robocalls cannot be reduced drastically. As already explained, the different authorities have to collaborate which is often a tedious process as legal documents have to be translated and routed via Interpol and through the various governments and law enforcement agencies (Harley, Grooten, Burn, & Johnston, 2012, p. 5). As the scammers are hiding their true identity and phone numbers the local victims barely have any usable information about the scammers. Because they are overseas, it is hard to trace and make a criminal case out of it. Also, the scammers often bribe the police, which is fairly common in a country that is rated by Transparency International as having serious corruption problems (Transparency International, 2019). In Malaysia where VoIP scams were among the top 3 cyber-crime cases in 2012, researchers found out that the current approach with awareness and safety campaigns by the government and private sector have to be proven as inadequate (Mubarak, Yahya, & Shaazi, 2019, p. 1). Many people perceive this as unsatisfactory, which leads to the idea of using additional security services and supplementary policing, which also use crowdsourcing methods as a new approach to combat cyber-crime more efficiently as there are individuals and organizations which have the expertise to make a material contribution to the investigative effort (Chang, Zhong, & Grabosky, 2018, p. 2ff; Shimomura & Markoff, 1996). Microsoft

already uses that approach by offering a website where people can submit information about tech support scams and then go through that data using advanced analytics to cluster the information to use it for their investigations and raids in India (Microsoft Digital Crimes Unit, 2018, p. 4). However, they are not the only ones: so-called scambaiters, individuals in online information communities specialized in identifying, documenting, and reporting actions of scammers, often using social engineering techniques and other more technical approaches in order to fight crime (Zingerle & Kronman, 2013, p. 1). They can be seen as anti-fraud activists and vigilantes, trying to raise awareness as well as doing community service (Zingerle & Kronman, 2013, p. 1). They use several tools to achieve their goals, e.g. using web forums as means to collaborate with other scambaiters and post information about the scammers and then submitting that information to Microsoft and law enforcement. An example of these websites or communities is scammer.info, with over 20,000 registered accounts, 30,000 threads and 120,000 posts (Scammer.info, 2020b). But they also need a tool to be able to call these scammer numbers as it is not advised to use the real phone number for several reasons: scammers may use the publicly available data that can be found on the internet when using the phone number of a person to call the police on the victim, falsely claiming that some violent crime is going on, so-called “swatting” (Elliot, 2016). They also might put the number on lists for other scammers to call and annoy them. That is why it is advised to use a secondary phone number or better use VoIP calling services.

This thesis’ objective is to analyze the use of crowdsourcing methods by scambaiters on scam call centers. As explained before, there are multiple ways to fight call center scams and robocalls and this thesis wants to assess if and how crowdsourcing methods can contribute to influence or obstruct activities of scammers and what motivations do the individuals have to do scambaiting in general, which goals do they have and why they are relying on crowdsourcing methods. Another important question is if the scammers feel an impact on their work due to the scambaiting and thus if crowdsourcing platforms function as a way to obstruct scammer activities.

1.2 Structure of the thesis

The introduction gives an illustration of the background and motivation of the thesis as well as an explanation of the structure of the thesis. Secondly, the theoretical

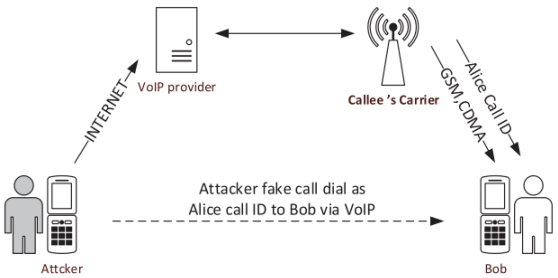
background, as well as the most important terms, will be explained. The method of the research consists of the general method, the case description, as well as the data collection and data analysis. In section four the findings will be presented. The discussion of the results will be treated in a further point. Lastly, the conclusion follows, based on limitations, future research topics, and a summary.

2 Theoretical background and terms

Many of the scam calls are from two different types of scam: imposter scams and tech support scams. Imposter scammers pretend to be from a government agency, usually the Internal Revenue Service (IRS) or the Social Security Administration (SSA), often using caller ID spoofing, to mislead the victim into paying money by using scare tactics such as threatening with an arrest warrant against the victim if he does not pay a fee to stop the proceedings (Bidgoli & Grossklags, 2017, p. 57; Gupta, Srinivasan, Balasubramaniyan, & Ahamad, 2015, p. 1; Tabron, 2016, pp. 13, 87; Tzani-Pepelasi et al., 2020, p. 163; US Department of Justice, 2020b, p. 5f). In this type of scam, the scammers use robocalls to transmit recorded messages to the phones and voice mails of the potential victims whose numbers they find in publicly available lists and phonebooks as well as so-called "sucker lists" – lists of previously scammed victims (Button, Lewis, & Tapley, 2008, p. 5; US Department of Justice, 2020b, p. 5f). Often in shock, the victims pay substantial amounts of money to the scammers using payment services such as MoneyGram, Western Union, and gift cards such as iTunes or Google Play Store cards as they are instant and non-refundable (Tzani-Pepelasi et al., 2020, pp. 163, 168; US Department of Justice, 2020b, pp. 5, 8). The scammers work in a team, with an "opener" reading a script and scaring the victim and a "closer" to persuade the victim to pay the money (Shover, Coffey, & Hobbs, 2003).

Caller identification (caller ID) is a service provided by the telephone carriers to show the call recipient who is calling (Mustafa, Xu, Sadeghi, & Schulz, 2014, p. 168). Caller ID services transmit the telephone number and/or the name of the caller to the recipient, but the existing protocols do not provide real authentication (Mustafa et al., 2014, p. 168).

Figure 2-1: Caller ID spoofing



Source: (Sukma & Chokngamwong, 2018, p. 1)

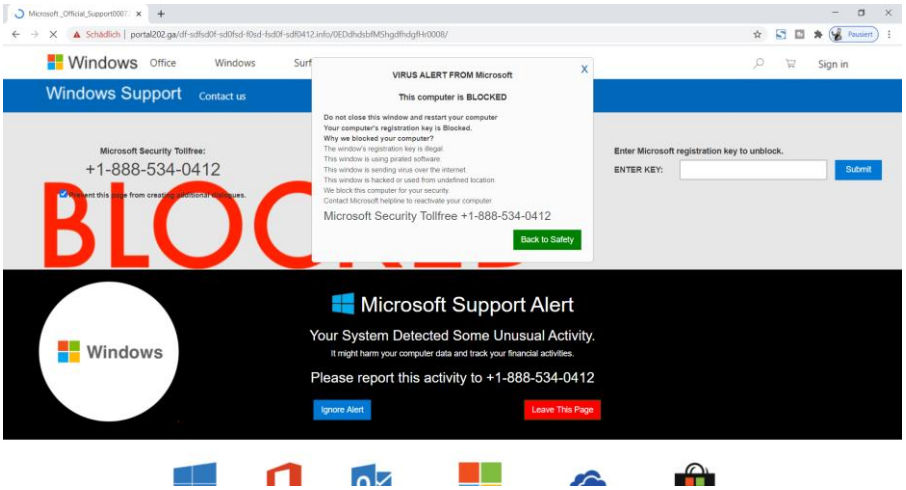
Since the caller IDs are transmitted in plaintext and with VoIP calling services allowing the customers to specify their own caller ID, this makes it easy to spoof caller IDs (Mustafa et al., 2014, p. 168f; Sukma & Chokngamwong, 2018, p. 1). Caller ID spoofing is illegal in the United States under the Truth in Caller ID Act of 2009 and the 2019 amendment, making it illegal to transmit misleading or inaccurate caller ID information with the intent to defraud (US Congress, 2009). Recent changes in the regulations by the FCC, namely the Standards Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN), phone carriers must verify if the caller ID is legitimate or spoofed and filter out the spoofed calls (FCC, 2019, p. 1). This is meant to stop fraudulent robocallers from sending out spoofed calls. Currently, the carriers are implementing this into their infrastructure (FCC, 2019, p. 2).

Researchers are trying to find ways of blocking these robocalls and unwanted calls. However, they have to overcome some difficulties they have identified, for instance, that calls are real-time and have an immediacy constraint (Tu, Doupe, Zhao, & Ahn, 2016, p. 324). That means the calls have to be analyzed and screened within a short window of time to avoid any delay that would make either the caller hangup or the recipient miss the call (Tu et al., 2016, p. 324). Another problem is caller ID spoofing, which makes it impossible for filtering services to rely on caller ID identification for blocking spam calls as the scammers and spammers can simply insert any random number as caller ID (Tu et al., 2016, p. 324). The researchers identified that no available technology alone manages to filter spam and scam calls effectively, requiring a combination of multiple technologies for an effective solution, for instance the “weighted scoring” method which produces a final score based on an assessment of various individual scores using different methods (Tu et al., 2016, p. 330). Another team of researchers used around 40,000 unused but “dirty” numbers (abandoned by the users because of the high volume of unwanted spam calls) to use them as a honeypot (Gupta et al., 2015, pp. 2f, 6). The goal was to analyze the incoming calls for a better understanding of telephony abuse and attacks and to gather empirical data (Gupta et al., 2015, p. 2). They measured a total of 1,297,517 unwanted calls over the course of 50 days that were made to 36,912 phone numbers they owned (some of their numbers did not receive calls at all), which results in approximately 0.70 calls per day per number (Gupta et al., 2015, p. 6).

Another interesting observation was that the call volume during US business hours and during week days was much higher than during weekend with 8,000 calls per day on weekends versus 33,000 per day on week days (Gupta et al., 2015, p. 6). Also, older phone numbers received more unwanted calls than newer allocated phone numbers which supports the idea of "sucker lists" meaning that older numbers are circulating for longer time among scammers and telemarketers as they sell those lists to each other (Button et al., 2008, p. 5; Gupta et al., 2015, p. 7f).

Tech support scams work differently. There are tech support imposter scams which also use outbound robocalls with recorded messages that claim the victim's computer has a virus or the allegedly previously purchased service plan is running out and is up for renewal or cancellation and ask for a call back in order to resolve the issue (Harley et al., 2012, p. 1; US Department of Justice, 2020b, p. 7). The typical tech support scam, though, uses a web page created by the scammer, also known as "fake pop-up messages", which typically tries to convince the victim that his computer is infected with a virus by using several ways of scaring the user (Miramirkhani et al., 2017, p. 1f; Tabron, 2016, p. 32). For instance, most of them use dramatic language and symbols to create urgency, sometimes even through an audio message that will be played once the popup is loaded (Miramirkhani et al., 2017, p. 7; Tabron, 2016, p. 32). To increase their trustworthiness, the scammers use the logos, trademarks, and generally the look of well-known software and brands (Miramirkhani et al., 2017, p. 2). Many if not most of these popups use intrusive JavaScript techniques to make it hard for the victim to navigate and close the page, e.g., by constantly showing alert boxes, reloading the page, or by creating a memory leak that freezes the browser (Miramirkhani et al., 2017, pp. 2, 7). The popup contains a call to action, asking the victim to "immediately" call the displayed telephone number, usually a toll-free number to increase the chance of the victim calling, so that the technicians can help him out (Javid & Chakraborty, 2019, p. 406; Miramirkhani et al., 2017, p. 2; Srinivasan et al., 2018, p. 320; Tabron, 2016, p. 31f).

Figure 2-2: Fake pop-up message



Source: (PopupDB, 2020)

Newer scam methods are using Search Engine Advertising (SEA) techniques to impersonate legitimate websites and even rank higher in the search results than the actual legitimate one, as well as scareware, typically fake antivirus software, that is promoting tech support scams inside the software (Miramirkhani et al., 2017, p. 14; Srinivasan et al., 2018, p. 326). Once the victim calls the toll-free number he will be routed to one of the scammers, a person claiming to be from Microsoft (sometimes they just answer using the generic term “tech support”) who wants to use remote access software such as GoToAssist or TeamViewer to connect to the victim’s computer to diagnose it (Miramirkhani et al., 2017, p. 2; Tabron, 2016, p. 34). Once they are connected, they use a multitude of methods and tools to convince the victim that indeed there is a virus infection on the computer and to gain trust for the following sales pitch (Javid & Chakraborty, 2019, p. 406; Miramirkhani et al., 2017, p. 2; Tabron, 2016, pp. 48, 52f). For instance, scammers show the Event Viewer, which shows many events, warnings, and error logs (Harley et al., 2012, p. 2; Miramirkhani et al., 2017, p. 10). However, all the shown errors are typical of any Windows installation and are no proof of a virus infection (Miramirkhani et al., 2017, p. 2). They also use terminology like “Koobface” or “Zeus trojan” in an attempt to establish their credibility as knowledgeable about computers even though they may not even use the technical terms in the right context (Tabron, 2016, p. 77f). Once the scammer managed to convince the victim enough that there is a problem with the computer, he will proceed to pitch the victim a paid service plan that is mandatory to remove the virus (Miramirkhani et al., 2017, p. 2; Tabron, 2016, p.

65ff). On average, the scammers request about $300, but some even charge $999 (Miramirkhani et al., 2017, p. 10f). Usually, the money is paid via credit cards which the scammers take over the phone or via a prepared web-shop (Miramirkhani et al., 2017, p. 2; Tabron, 2016, p. 46). Usually, scammers work in organized call centers, and similar to the IRS/SSA scam call centers use several roles: sales agents and technicians (Button et al., 2008, p. 16f; Miramirkhani et al., 2017, p. 11). As per the size, in the study by Miramirkhani et al., the average amount of employees was 11 with up to 19 sales agents reachable on one phone number, however their number can be also bigger (Miramirkhani et al., 2017, p. 12).

Crowdsourcing is a relatively new concept that is a neologism of the words “crowd” and “outsourcing” and means the outsourcing of creative and work processes and insourcing knowledge, capital, and time into an organization (Pelzer, Wenzlaff, & Eisfeld-Reschke, 2012, p. 13; Schall, 2012, p. 8; Tucci, Afuah, & Viscusi, 2018, p. 2). It is a flexible and highly scalable solution to solve tasks that cannot be automated and require contextual thinking of a human and is highly cost-effective, promising a cost reduction up to 90% in comparison to in-house solutions or traditional outsourcing (Pelzer et al., 2012, p. 20; Schall, 2012, p. 8). Crowdsourcing can appear in various forms: engagement & charity, microworking & tasks, collective knowledge, creative content marketplaces, open innovation & ideas, and crowdfunding (Pelzer et al., 2012, p. 20). In some forms, there is no financial compensation for the user (Pelzer et al., 2012, p. 48; Tucci et al., 2018, p. 18). That is especially the case for NGOs and other social activist and non-profit projects or organizations as the motivation of the user is to be part of the project and to contribute something to the common goal (Pelzer et al., 2012, p. 48). Often-times, fame, honor, or appreciation are important motivations as well (Pelzer et al., 2012, p. 48). Another motivation can be entertainment or simply fun (Pelzer et al., 2012, p. 48). Entertainment and fun can be achieved by using gamification elements such as awarding users XP points so that users can compete with other users (Pelzer et al., 2012, p. 80). Collective knowledge for instance means the collection and creation of knowledge by individuals in groups with a common interest using IT infrastructure (Pelzer et al., 2012, p. 23). Crowdfunding, as form of crowdsourcing, means the collection of funds for e.g., artists, startups, or NGOs using the crowd (Pelzer et al., 2012, p. 34; Tucci et al., 2018, p. 97f). It is particularly important for those who do

not have access to more traditional sources of finance (Dushnitsky & Marom, 2013, p. 24). Crowdfunding for NGOs or charities are also called crowd donations and are usually without any consideration but also can have some small service or goods in return (Pelzer et al., 2012, p. 34). There are four sub-categories of crowdfunding: donation-based where the donors are motivated by social or intrinsic aims and receive mostly intangible benefits in return, rewards-based where the contributions are a form of pre-purchasing a product or service, equity-based where the donations are given in the form of equity investments, and peer-to-peer lending where the contribution acts as a loan and has to be paid back (Dushnitsky & Marom, 2013, p. 25). The donors are usually integrated into the project or organization in some way, for example, as a source of inspiration for future features or simply as a user (Pelzer et al., 2012, p. 34; Tucci et al., 2018, p. 98). Microworking & tasks are used in various fields such as editing and proofreading, translating texts, tagging of images, video- and audio files (Pelzer et al., 2012, p. 20; Schall, 2012, p. 1; Tucci et al., 2018, p. 13). A similar form is online-volunteering which is targeting mainly users who want to engage with NGOs but are not able to work at the location due to various reasons (Pelzer et al., 2012, p. 41). To plan the outsourced tasks, there should be a description of the goals, the required competencies, and the available resources as well as the time frame for the completion of the tasks (Pelzer et al., 2012, p. 43). The benefits for the organization of crowdsourcing are not only the cost reduction but also the scalability, an increased pool of ideas and innovations, and unbureaucratic on-demand solutions (Pelzer et al., 2012, p. 49; Tucci et al., 2018, p. 17f; Vanhaverbeke, Vermeersch, & De Zutter, 2012, p. 9). It can be noted that also a certain level of quality is ensured due to multiple users competing, striving for better results, and double-checking on existing ones (Schall, 2012, p. 7). For the user the benefits are flexible time management, the location-independent mode of working, an increase of reputation and appreciation of the community, new contacts, and fun (Pelzer et al., 2012, p. 49). Crowdsourcing can also be used for research and journalism: as displayed in the GuttenPlag Wiki case, thousands of users were able to collaborate online to solve one big task (Pelzer et al., 2012, p. 66). Their motivation was to fight for the same thing or, as Dirk von Gehlen, chief editor of jetzt.de, puts it: “A bogeyman is always the best connecting link” (Pelzer et al., 2012, p. 66). There are some dangers involved in this also: an expert has to verify the results to make sure no mistakes happened (Pelzer et al., 2012, p. 67). Another disadvantage of

crowdsourcing is that the problem may not be formulated well enough for the users to understand it, resulting in a wrong solution or no solution at all (Tucci et al., 2018, p. 19). In regards to telephone scams, crowdsourcing can be used to get datasets of telephony abuse: users report fraudulent scam numbers on websites such as 800notes.com or scammer.info, and these sites will be used to warn other potential victims of the scam who receive a call from this number and are searching online what kind of call it is (Gupta et al., 2015, p. 1). Crowdsourcing can also be used for the co-production of cyber security: the increase of digitalization of our lives leads to an increase of potential crimes (Chang et al., 2018, p. 101f). Many of these crimes online are being unreported or are ignored by law enforcement, often due to a lack of resources and interest (Huey, Nhan, & Broll, 2013, p. 82). That is why there is a demand for supplementary policing and security services that could be met through collaborative efforts of plural actors, so-called nodal clusters (Chang et al., 2018, p. 101f). Research has been done on phone scam activities in Malaysia, including their impact, scam tactics, and possible prevention methods, stating that current preventive methods by private sector players and government bodies are still inadequate, and it does not appear that the scams will end anytime soon (Mubarak et al., 2019, p. 1). The new approach with nodal clusters includes criminal investigators, private industry players but also individual internet users, with some of them forming voluntary ad hoc partnerships with law enforcement (Chang et al., 2018, p. 102; Huey et al., 2013, p. 83). It can also include vigilantism (netilantism) and even white hat hackers (“good” hackers) (Chang et al., 2018, p. 103). The possible activities can range from passively increasing their own security to avoid being victimized over reporting suspicious activity online and grouping in online forums and communities, conducting investigations on their own of illegal activities, using social-engineering tactics, and also actively assist the authorities (Huey et al., 2013, p. 83; Wall & Williams, 2007, p. 403; Zingerle & Kronman, 2013, p. 352). These individuals are so-called scambaiters (Zingerle & Kronman, 2013, p. 352). For instance, in March 2020, the scambaiter and YouTuber Jim Browning uncovered a scam call center operation in Delhi, India, and provided valuable information and evidence to the authorities, which lead to the arrest of the call center owner (BBC Panorama, 2020). In these online communities, each individual actor brings their own form of capital: *economic capital*, which refers to the monetary resources, *political capital*, which refers to the individual’s ability to influence public policy and use government

resources, *cultural capital*, which refers to specialized knowledge, *social capital*, which refers to the ability to create and maintain mutually beneficial social relations with others, and *symbolic capital*, which means institutional legitimacy and therefore directs the other forms of capital (Huey et al., 2013, p. 83f). The integration of the capital of the various individuals for a common goal often results in much faster investigation results than law enforcement organizations are achieving (Huey et al., 2013, p. 94). Another advantage is the broad range of capital and including the time that the individuals spend (Huey et al., 2013, p. 94). Time is perhaps the greatest resource the civilian policing group members have, meaning the time spent on research, visiting the online communities, posting and more (Huey et al., 2013, p. 90). The scambaiters' motivation can range from community service to revenge for being victim of a scam in the past (Zingerle & Kronman, 2013, p. 352). Some researcher comes to the conclusion that a major motivation for scambaiting Nigerian Advance Fee Fraud, also known as "419 email scam", is racism, which is a controversial claim as other researchers identified altruism as possible motivation (Nakamura, 2014; Zingerle & Kronman, 2013, p. 352f). Those online scambaiting communities even often have ethical codes (Zingerle & Kronman, 2013, p. 353). Zingerle & Kronman identified and categorized seven types of scambaiters for the Nigerian 419 scam, based on their activities, techniques, legality aspect, and motivation: the *scam alerters*, which identify scams and warn vulnerable people by creating forums and FAQs, the *trophy hunters*, which try to bait the scammer while aiming for a so-called "trophy" – usually a photo the scammer took of himself in an unusual setting, the *website reporters*, which report scammer websites to the corresponding hosting providers in order to shut the websites down, the *bank guards*, which try to identify the bank accounts the scammers are using and then they approach the banks and law enforcement to close the accounts and the monetary stream, the *romance seekers*, which are basically scambaiting romance scammers in order to gather evidence to warn potential victims, the *safari agents*, which try to make the scammer travel at least 200 miles or cross borders to another country, and lastly the *inbox drivers*, which try to get into a scammer's email account in order to monitor the activities and warn potential victims with whom the scammer is in contact with (Zingerle & Kronman, 2013, p. 353ff). In terms of phone scambaiting, such as tech support scam or IRS/SSA scams, scambaiters call the scammers to keep them on the phone and to waste their time as long as possible so that real victims will

be kept from harm (Tzani-Pepelasi et al., 2020, p. 166). Not all law enforcement agencies are regarding this development as positive: legal liabilities associated with civilian involvement in investigations may be an issue as well as the perceived information quality being questionable (Huey et al., 2013, p. 94f). While this may be in some cases, certainly in other cases the information provided by the individuals has been proven to be crucial and groundbreaking and thus are currently a much undervalued cluster in the cyber-space security network (BBC Panorama, 2020; Huey et al., 2013, p. 95). Microsoft already uses that approach by offering a website where people can submit information about tech support scams and then goes through that data using advanced analytics to cluster the information to use it for their investigations and raids in India (Microsoft Digital Crimes Unit, 2018, p. 4). As previously explained, there is research about various aspects of the scams, fighting scams, crowdsourcing, and scambaiting. However, there is a gap in research as to how crowdsourcing is being used for scambaiting and how specific platforms can contribute.

3 Method

3.1 General method

This thesis is a case study. A case study can be defined as an intensive study about a person, a group of people or a unit, which is aimed to generalize over several units and be either illustrative or confirmable (Gustafsson, 2017, p. 2). Case studies are also used to develop theories about several topics (Eisenhardt & Graebner, 2007). They are open-ended and often used in situations where it is hard to find a precise solution or when the focus is on a contemporary phenomenon within some real-life context and contributes to our knowledge of the individual, group, organizational, social, political, and related phenomena (Gustafsson, 2017, p. 5; Yin, 2003, p. 1). They exist as a single case and multiple case studies, but since the aim of the thesis will be to analyze one crowdsourcing tool in particular, the format of the case study has to be a single case study (Gustafsson, 2017; Yin, 2003). The mode of research of this thesis is qualitative research. Qualitative research is needed to answer research questions that address the "how" and why" in unexplored research areas particularly well (Eisenhardt & Graebner, 2007, p. 26; Yin, 2003, p. 1). Qualitative case study research is a flexible method (Merriam, 2009), and case studies are one of the best methods to use qualitative evidence and get to mainstream deductive research (Eisenhardt & Graebner, 2007, p. 25). In this case, the interviews will be conducted to answer these types of questions about the case, and thus, qualitative data will be collected.

3.2 Case

The case will be the crowdsourcing VoIP tool "BobRTC", accessible under bobrtc.tel (Discommunications LLC, 2020). It is a web-based phone dialer, based on webRTC technology, which is a relatively new technology based on HTML5 that allows real-time communication functionality within the browser and thus does not need any third-party software to be downloaded or installed (Rodríguez, Cerviño, Trajkovska, & Salvachúa, 2012, p. 180; Sredojev, Samardzija, & Posarac, 2015, p. 1006). This technology is supported by major companies such as Google and Mozilla, and because of that, the vast majority of browsers are supporting it, making BobRTC available on many devices (Sredojev et al., 2015, p. 1006). On the server-side,

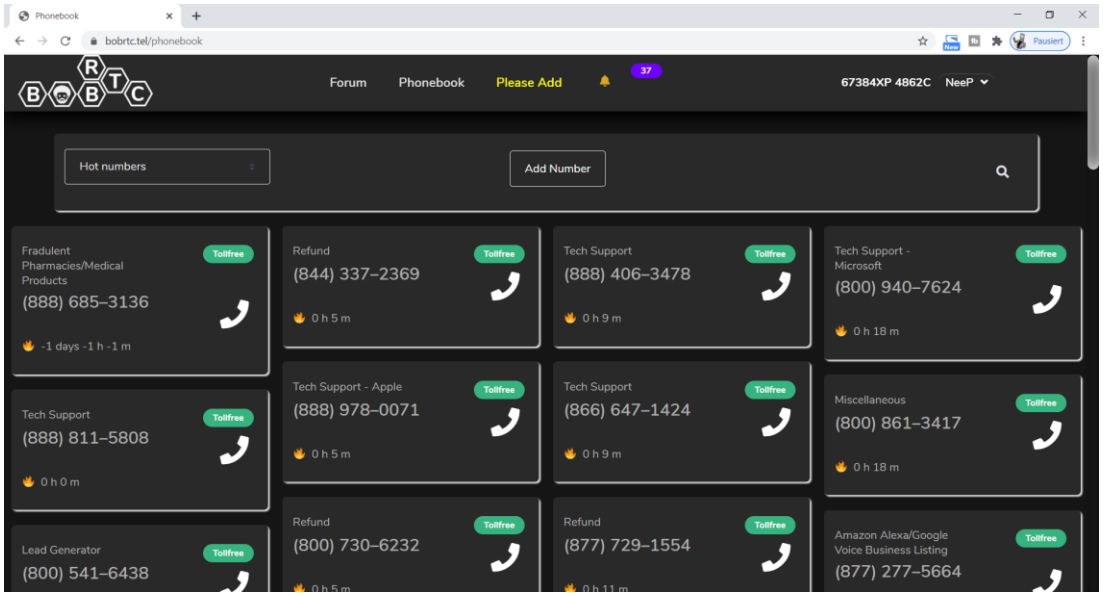
BobRTC is based on a conventional Asterisk phone server, using the previously explained webRTC technology to relay the audio to the browser clients.

BobRTC is designed to be used to combat telephone fraud by letting any registered user call scammers and waste their time or using the service to extract information out of the scammers over the phone call or simply do prank calls. The principle is similar to conventional VoIP tools such as Skype but with some major differences which will be explained further on. Currently, it has over 33,000 user accounts. The website and its use are completely free for users. The tool consists of two main screens:

First, there is the “phonebook”. It is a list of scammer numbers that have been either manually added by users and moderators, or they have been automatically imported to the phonebook by a bot using APIs of various number reporting websites and tools such as RoboKiller, an app that crowdsources scammer numbers from phone users and has over a million installations (Google Inc, 2020; Teltech Systems Inc, 2020). The manually added numbers will be verified by the moderation team to make sure that the numbers are actually related to scammers and robocallers and not to genuine and legitimate businesses to prevent abuse. Most available scammer numbers are United States-based phone numbers; however, British, German, Australian, and French numbers are also supported because these are the countries that are targeted by the scammers. Also, the numbers are added to scam type categories which allow the users to filter by a specific type of scam, for instance just IRS/SSA impostor scams or tech support scams, based on the preferences of the user. It is also possible to search for a specific number. Only those numbers which are added and verified will be available to call.

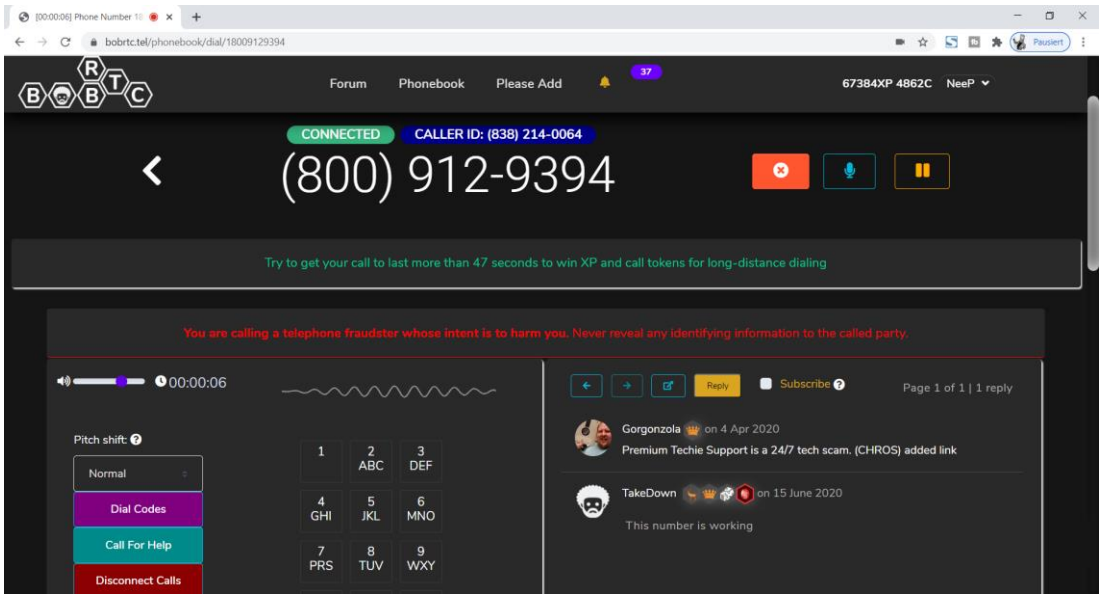
Once a user clicks on a number, it will open the second main screen, the “dial page”. On this page multiple items are shown, such as the scammer number, the type of scam, and a field for details to this specific scammer number. The users can use this field to name the scam company or give valuable information or insights, tips and tricks on how to bait this particular scammer and more. The page has the standard set of buttons for a phone system, such as a dial pad, a dial and hangup button, and also a mute button. Below the dial pad, there is an Internet Relay Chat (IRC) which allows the users to chat with each other in real-time.

Figure 3-1: BobRTC phonebook



Source: (Discommunications LLC, 2020)

Figure 3-2: BobRTC dial page



Source: (Discommunications LLC, 2020)

What makes it different from conventional VoIP tools such as Skype is that it is based around scambaiting. It is not possible to call any number of the user's choice. The system is locked down to manually confirmed scammer phone numbers in the phonebook to prevent misuse and harassment of individuals or legitimate businesses. Other scambaiting-specific functions are an auto-redial button, which dials a number

again once the scammer has hung up the phone to speed up the process of calling scammers when they disconnect the phone quickly. Another feature is the voice bots, which are pre-recorded audio snippets of a person, which will be played on the phone call, making the scammers believe that someone is talking to them. One of the most important features is the caller ID spoofing, which means that each outgoing call will be faked to have a different caller ID displayed to the scammer, making it look like BobRTC is calling from different numbers even though it does not own them (Federal Communications Commission, 2019, p. 2; Mustafa et al., 2014, p. 168f; Tu et al., 2016, p. 323f). This makes it impossible for scammers to block the calls as the caller IDs are randomized and can be any number. This is a feature that greatly differentiates BobRTC from conventional tools such as Skype, which calls from a small pool of caller IDs, which are known to the scammers and can be blocked easily. However, due to the STIR/SHAKEN regulation, BobRTC is using a big pool of unused telephone numbers that have been leased from telephone carriers, and because these numbers are owned by BobRTC, it is able to set the caller ID as these phone numbers. As the pool of numbers is so big, it is still hard for scammers to block the BobRTC calls. The pool of numbers is exchanged frequently to further improve the capabilities of BobRTC.

BobRTC is a crowdsourcing platform that relies on the number of users to add new scammer numbers as old ones get deactivated either by the scammers themselves or due to reports to the respective phone carriers. BobRTC encourages users to add numbers to the phonebook and to call scammers by awarding each user with experience points (XP) for each number added and for each minute called. This XP will be collected and with a certain amount, can unlock new features. There is also a leaderboard which makes it able to compare one to another by the amount of XP.

As already explained previously, BobRTC is completely free for the user, but it is using crowdfunding to finance the costs for the project, such as the infrastructure and also the phone calls. Users can donate to BobRTC on a monthly basis and receive some goodies in return for their support. That way, the costs are getting covered while still be appealing to many users who do not want to spend money on scambaiting or are still minor and thus not in possession of a credit card or other payment methods.

3.3 Data collection

As data collection method, expert interviews will be used to get a holistic understanding of the situation to get the different views and experiences of the individual interviewees to answer the research question as they have answers to all the questions (Gläser & Laudel, 2010, p. 11). Expert interviews are a form of qualitative interviews, but with a special target group (Lamnek, 2010, p. 656). Experts are not only individuals in high-ranked positions but also users who have lots of knowledge or experience in a certain field (Gläser & Laudel, 2010, pp. 11f, 43; Lamnek, 2010, p. 655f). It is also possible to conduct group interviews with experts, but in this case, individual interviews will be conducted (Lamnek, 2010, p. 655). Several types of expert interviews can be distinguished after Bogner & Menz (2005): explorative expert interview, systematizing expert interview, and theory generating expert interview (Lamnek, 2010, p. 656). In this study, the systematizing expert interview will be chosen as it focuses on practice-based knowledge and experience (Lamnek, 2010, p. 656).

A total amount of nine interviews will be conducted from two groups: one group is the BobRTC users. Five experienced and highly knowledgeable users will be chosen using purposeful sampling from the total of 33,000 users the platform currently has, to view the phenomena from diverse perspectives (Eisenhardt & Graebner, 2007, p. 4; Gläser & Laudel, 2010, p. 117; Merriam, 2009, p. 77). In this case, the interview partners were selected from the top 50 users of BobRTC based on their XP amount, which reflects the experience and time spent using this platform. Field access is supported by the administrators of that platform (Lamnek, 2010, p. 657).

The other group is the scammers. Four scammers that were recruited using convenience sampling will be chosen, which have to have experiences with calls from scambaiters using crowdsourcing methods (Merriam, 2009, p. 79). They are or were working in different scam call centers and locations across India, including Delhi, Chandigarh, and Kolkata. Most of them work or worked in tech support scam call centers. One worked in a Social Security Administration scam call center, with the difference that, in contrary to tech support scam call centers, this is a phone-call-only scam, meaning less technical knowledge is required by the agent. They all agreed to participate in the thesis as long as their identities are not disclosed.

The two-sided interview approach will allow for a better understanding because more involved parties are being questioned. The number of interviewees was chosen, taking feasibility into account as well as the minimum amount of interviews to get basic information (Gläser & Laudel, 2010, p. 104). The interview technique is the non-standardized interview with the subtype guided, semi-structured interview, using a list of open, predefined questions which will be used to stimulate the conversation and further, more detailed questions will follow spontaneously and in a natural flow with the conversation (Gläser & Laudel, 2010, pp. 43, 111f; Merriam, 2009, p. 89f). An individual questionnaire will be used for each group of experts because of their different roles in the observation and to capture their specific knowledge (Gläser & Laudel, 2010, p. 117). When creating the questionnaire and selecting the individual questions, the "SPSS" approach by Helfferich (2005) was used, meaning a four-step approach which includes firstly collecting as many questions as possible, then checking if the questions are suitable to find answers to the research question, followed by sorting the questions and finally subsuming them (Helfferich, 2005, p. 161f; Lamnek, 2010, p. 321f). Very important for these steps is also the principle of openness of questions to give room to the various answer possibilities of the interview partners to allow them to share their experiences and knowledge as well as possible (Gläser & Laudel, 2010, p. 115f; Lamnek, 2010, p. 322). The questionnaire will start with background and demographic questions to learn more about the interviewee, and then experience and behavior questions, opinion and value questions as well as knowledge questions will be used (Gläser & Laudel, 2010, p. 122ff; Merriam, 2009, p. 96f). Also included in the questionnaire prior to the questions itself is an introduction to explain the topic of the thesis to the interviewees as well as a declaration of the data protection rights (Gläser & Laudel, 2010, p. 54). Research can affect people's lives e.g. by publishing the results (Gläser & Laudel, 2010, p. 48). The interviewees have the rights to be treated under the fundamental ethical principles of society so in this case, it means that the private or identifiable information will not be shared with any third parties to avoid any damages or problems for them (Deutsche Gesellschaft für Soziologie & Berufsverband Deutscher Soziologinnen und Soziologen, 2017, p. 2; Gläser & Laudel, 2010, p. 49f). That is especially important for the second group of interview partners, the Indian scammers, as they are breaking the law on a daily basis in their job, which could result in prosecution if their data would become public or shared. The interviews are

conducted over a voice call because a written interview would violate the central principles of qualitative research: openness and flexibility (Gläser & Laudel, 2010, pp. 30, 42f; Lamnek, 2010, p. 313). A benefit of voice calls as a method for conducting the interviews is the wide geographical access: people from all over the globe can be interviewed which is a crucial point considering that the nine interviewees of this thesis are from four different countries on four different continents (Opdenakker, 2006, p. 4). It would be simply too expensive and would consume too much time to travel to each individual interviewee to conduct face-to-face interviews (Opdenakker, 2006, p. 4). A drawback of voice communication is that it is not possible to see visual information such as facial expressions that would add context to a statement of the interview partner. However, as explained, in this case study it is simply not feasible to travel to each individual interview partner (Gläser & Laudel, 2010, p. 153).

Table 3-1: List of interviewees

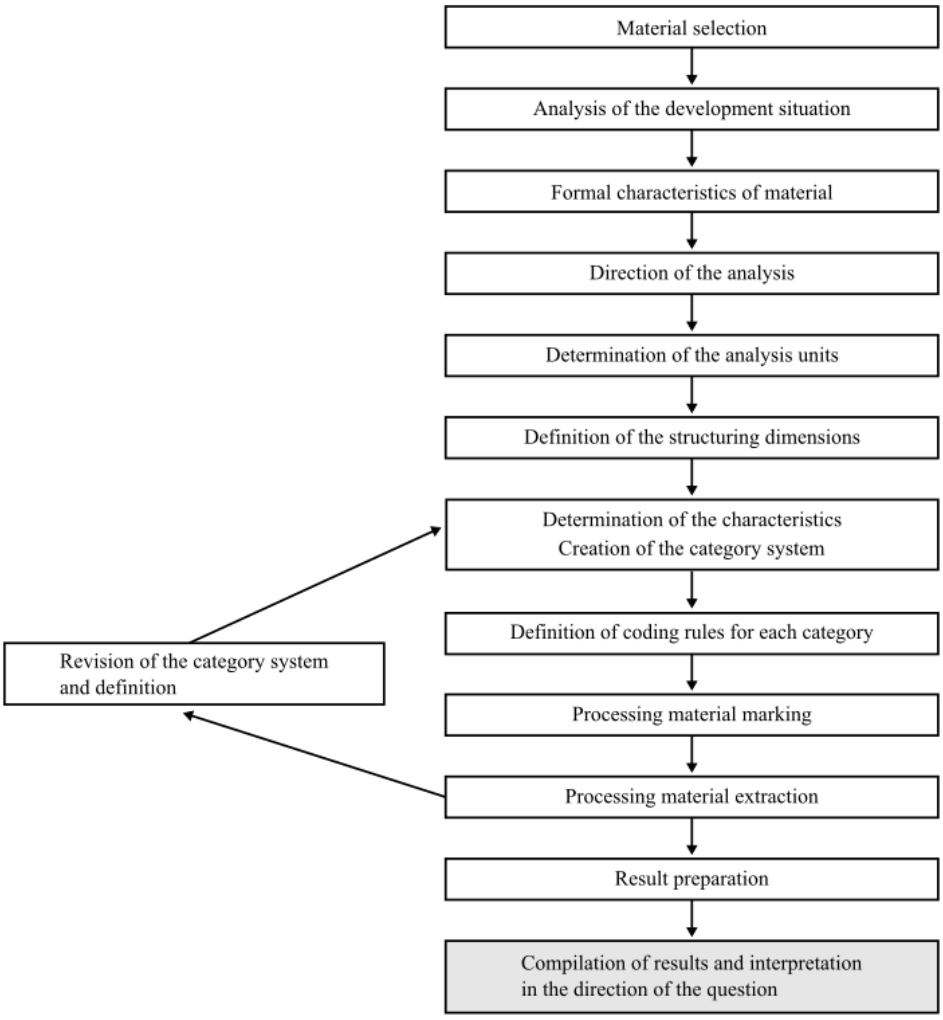
ID	Interview Partner	Gender	Position/Background	Experience	Mode of interview	Interview Duration
B1	Scambaiter 1	Male	Very experienced scambaiter both on BobRTC and on scammer.info. Indian origin but living in the US; mainly calling and researching about the scammers	3y 6m scambaiting, 1y 3m BobRTC	Discord audio call	37m 39s
B2	Scambaiter 2	Male	Top30 user based on XP on BobRTC and part of the moderation team on the platform, adding new numbers and verifying submitted numbers of other users	5-6y scambaiting, 1y 3m BobRTC	Discord audio call	42m 39s
B3	Scambaiter 3	Male	Part of the BobRTC admin team, developing bots and API integrations as well as managing web hosting and other tech related issues	2y scambaiting, 1y 3m BobRTC	Discord audio call	48m 36s
B4	Scambaiter 4	Male	Top30 user based on XP on BobRTC from Australia;	4y scambaiting, 1y 2m BobRTC	Discord audio call	18m 37s
B5	Scambaiter 5	Male	User from UK, strong IT background, focuses more on researching and investigating the scammers	3-4y scambaiting, 6m BobRTC	Discord audio call	53m 15s
S1	Scammer 1	Female	Working in tech support scam call center in Delhi, targeting Germany, graduated, B1 level German language	6m work	Skype audio call	16m 29s
S2	Scammer 2	Female	Worked in an IRS and refund scam call center based in Kolkata; targeting US Americans, now working as Teamleader in legitimate company	1y work	Discord audio call	34m 13s
S3	Scammer 3	Male	Worked in a tech support scam call center in Chandigarh, targeting US Americans; provided a lot of insider information in the past	6-12m work	Discord audio call	23m 34s
S4	Scammer 4	Male	Worked in a tech support scam call center in Chandigarh, mainly as technician – not in sales too much, provided a lot of insider information in the past	3y work	Discord audio call	39m 59s

The calls were mostly conducted over Discord, a chat application with voice/video call functionality, which is extremely popular among the BobRTC users, as well as over Skype. The calls were recorded locally on the interviewer's PC. These audio recordings of the interviews have to be transcribed to be analyzed (Mayring, 2015, p. 55). That is why the audio recordings were uploaded to an automated transcription website named Sonix.ai. The software automatically transcribes audio to text while also separating the individual speakers. Because the software is not flawless, and the terminology used in the interviews is not standard dictionary vocabulary, the transcription results have to be corrected manually. During this step, the text will be edited to increase readability (Mayring, 2015, p. 55). Filling words such as "uhm" as well as duplicate words and stutter will be removed but keeping the result as close as possible to the original interview. The transcripts of the interviews are included separately as digital copy.

3.4 Data analysis

Data analysis is the process of making sense out of the data, including the analysis of communication content, to answer the research question (Merriam, 2009, p. 175f; Mollenhauer & Rittelmeyer, 1977, p. 185). This involves consolidating, reducing, and interpreting what people have said and what the interviewer has seen and read (Merriam, 2009, p. 175f). Using that data, inductively, a process is derived which identifies the factors that answer the research questions (Merriam, 2009, p. 176). This process is based on explicit rules to meet socio-scientific standards (Mayring, 2015, p. 12f). This thesis follows the content analysis model of Mayring (2015), specifically the structuring content analysis, which tries to extract and filter out certain themes, contents, and aspects out of the material and to summarize it (Mayring, 2015, p. 103). The process consists of these steps:

Figure 3-3: Process model of structuring content analysis



Source: (Mayring, 2015, pp. 62, 98), adapted

The process starts with finding relevant materials (Merriam, 2009, p. 150). During the analysis, it is only allowed to add or modify the material under certain justifiable necessities (Mayring, 2015, p. 54f). Here, the edited transcripts of the nine interviews will be the material. Due to the difference in perspective, the process will be conducted individually for each group, the scambaiters and the scammers. Then, the development situation has to be analyzed: especially the socio-cultural background and the persons involved in the creation are important (Mayring, 2015, p. 55). In this case, this has been done by describing each participant in Table 3-1, for instance their working experience, their background and education. The next step is the formal characteristics of the material. According to Mayring (2015), this does not only include the recorded interviews, transcribed to text, but also metadata such as observation data or other text-based data (Gläser & Laudel, 2010, p. 210; Mayring,

2015, p. 55). For this thesis this does not apply, as there are no recorded observations. Going forward, the direction of the analysis has to be defined. This can be done using the Lasswell formula for the analysis of communication as aid (Mayring, 2015, p. 58). In the thesis, the direction would be the subject: the goal is to find out about the case BobRTC. Now, to increase the precision of the content analysis, the structuring dimensions will be specified: the coding unit, which is the smallest unit that can be categorized, will be defined as words (Mayring, 2015, p. 61). As context unit, which is the biggest unit that can be categorized, will be defined as paragraph (Mayring, 2015, p. 61). The evaluation unit will be set as the full material for each group, meaning five interviews for the scambaiters and four for the scammers (Gläser & Laudel, 2010, p. 209f; Mayring, 2015, pp. 61, 88). Next, the structuring dimensions have to be defined. Mayring (2015) states that they have to be derived from the research question as he is using a deductive method, however, in this thesis an inductive method is used, deriving the dimensions from the material itself (Mayring, 2015, p. 97). The following steps are an iterative process where the actual analysis is happening: the characteristics have to be determined and the category system created (Mayring, 2015, p. 97). The next step is called “coding” which means assigning some sort of shorthand designation to various aspects of the data so that it is possible to easily retrieve specific pieces of data (Mayring, 2015, p. 97; Merriam, 2009, pp. 173, 178f). That designation can be single words, letters, numbers, phrases, colors, or a combination of these (Mayring, 2015, p. 97; Merriam, 2009, p. 173). These will be marked with different colors throughout the text (Mayring, 2015, p. 99). Through the assignment of codes, categories will be constructed (Merriam, 2009, p. 179). It is important that the created category system has to be examined and reviewed to make sure that it still answers the research question (Mayring, 2015, p. 98f). The found references in the material which are coded have to be extracted according to each category (Mayring, 2015, p. 98). The results will be then prepared and interpreted according to the direction of the research question (Mayring, 2015, p. 62). PC software is being used to aid in this process as it is much easier to do and to visualize the coding process (Mayring, 2015, p. 115ff). Specifically, MAXQDA was chosen (MAXQDA, 2020). As per the compilation of the results, no adequate literature was found that would provide steps or guidelines regarding that.

4 Findings

The analysis resulted in a total of seven code sets and categories used to answer the research question and 166 coded segments over the nine interviews. The final categories are *"motivation"*, meaning the motivation of the BobRTC users for scambaiting in general, *"scambaiting activities"*, meaning all the activities scambaiters would do in order to fight call center scams, *"useful features"*, meaning the features of BobRTC that were mentioned as particularly useful for scambaiting activities, *"security/privacy"*, meaning ways of protecting the users identity and keeping the user from harm from the scammer, *"crowdsourcing aspect"*, meaning all the features or aspects of BobRTC that would fall under different variants and aspects of crowdsourcing, *"perceived impact"*, meaning the impact that the scambaiter thinks his action has on scammers, and lastly *"actual impact"*, meaning the impact it has from the perspective of the scammers.

The motivation of the BobRTC users for scambaiting consists of three themes: stopping scammers from hurting people, curiosity in criminal phenomena, and diversion. B1, for example, stated that his motivation was to do something because his fellow American and Indian would be hurt by the deeds of the scammers. He also states he has plenty of time, which seems to be a theme across all interviewed scambaiters, which state they spend several hours daily on scambaiting. B3's grandmother got scammed by tech support scammers, and he wants to take revenge as well as protect her from future scams. B5 shows interest and curiosity in how the scammers operate, how they make money and how exactly they scam people. Another motivation for him is diversion. He states it is enjoyable and fun. B4 joins the theme of stopping scammers while also enjoying the calls. Interestingly, the scammers often have a different perception: they usually do not use the term "scambaiter" but rather "prank caller". S1, for example, states that she thinks that the scambaiters let the scammers connect to their computers to prank them. S2 and S3 realized that some scambaiters might have a motivation to stop the scams from happening.

The scambaiting activities follow a very broad spectrum, which can be categorized into raising awareness, research & reporting, prank calling and time-wasting, support & administration. The categories are not exclusive. Often, scambaiters combine multiple categories. For instance, B5 says he is calling scammers and posing as a

victim to waste their time; however, he also states he is gathering information, investigating, and then reporting it to the authorities and companies to get the scammers arrested and their websites and phone numbers taken down. B3 started with calling scammers and doing research on scammers, which he would publish on scambaiting forums such as scammer.info, but now he moved to the support & administration category, essentially developing tools for the scambaiting community. B2 usually searches for scam numbers and shares them on social media, for other scambaiters to call, and he calls scammers in a group call with a friend. B1, being of Indian origin, analyzes the accent of the scammers on the phone, trying to locate them and posting that information on scambaiting forums. Again, the scammers have different views: S1 and S4 say the scambaiters are calling and using abusive language. S2 recalls an incident where a co-worker of hers got scambaited and the call live-streamed on YouTube. In another incident, a scambaiter tried to scare her by threatening to leak her personal details online.

When being asked about useful features of BobRTC several functions are being named: one of the most named features was the phonebook. B1 reasons this as its dropdown menu of scam types are well-defined, meaning that it is easy to choose a particular type of scam to call. B2 adds that it is very convenient as it is not needed to spend time on finding scammer numbers. This can also be a disadvantage, as he adds later on: these numbers are the only ones that can be dialed – BobRTC does not have a free dial pad for legal reasons. To compensate for this, B3 explains that BobRTC uses APIs to automatically import phone numbers off RoboKiller, a spam call blocking app which crowdsources its database from the customers' phones. This way newer phone numbers will be added and available to call. The same integration happens with PopupDB.org, a website that automatically analyzes fake pop-ups and extracts the phone number out of it. Another feature are the voice bots. B3 finds them funny but also useful because they are designed to carry on a conversation for as long as 40 minutes and this is all automated. B5 found another use case: to scambait new types of scam where he does not know how the scam works. He will learn from the answers and questions the scammer is asking the bot. B2, on the contrary, does not use them really as he prefers to talk to them in his real voice. From the scammers, S4 remembers having had a call from the voice bot named Lenny. The Auto-Redial function is also liked. B2 says it helps to save time as it instantly calls the scammers

again once the call is dropped, and B5 adds convenience as a benefit. The possibility of leaving comments on each scammer number is a feature that specifically B1 likes to post his research on scammers. Definitely, the most mentioned feature is the caller ID changing. B2, B4, and B5 say BobRTC is much better than conventional services as those do not provide a new caller ID on every call. If scammers block the number, it is not possible to call them again. With BobRTC, however, due to his caller ID changing on every call, it makes it impossible to block the calls, which means he can scambait them for longer. B1 requests the feature to be changed so that a specific caller ID can be chosen by the user. B3 explained that the caller ID used to be spoofed previously but now is chosen from a pool of 40,000 phone numbers that are leased by BobRTC for that purpose. The XP point system has received mixed reactions: B2 does not fully understand the benefits of the XP for himself. B3 explains that the more XP a user collects, the more features he can access, like the Dial Party. B4 recognizes the function of the XP system, but he has unlocked all the features already and sees it rather as status. B5 does not see any fun in the current XP system, but he suggested implementing achievements or medals which can be unlocked on certain events such as 100 minutes of scammer time wasted. As a missing feature, B2 mentions a voice chat that would allow scambaiters to talk to each other so that new users could get advice from the community on how to use the tools and how to do scambaiting in general.

The security and privacy features are also playing a big role: B1 states he is worried about his relatives in India because of his scambaiting activities. BobRTC is hiding his identity behind a fake caller ID, which makes him anonymous to the scammers. B2 adds that no personal information is required to provide when using or registering for the platform, so even to the platform itself, the user can be anonymous. He also adds that it is very convenient as it is built right into the platform, and the user does not need to do anything. B3 explains that it is rare that scammers use lawsuits against scambaiters as they would have to expose their own identity for that, but it does happen. In this case, having BobRTC in between and not a regular company like Google (Voice) or Microsoft (Skype) is a benefit as there is no real information stored on BobRTC. B4 adds that he uses a virtual private network (VPN) when he is baiting tech support scammers to leave even fewer clues behind. B5 is not

particularly scared of any consequences as the scammers are the criminals and so far away but he is still using BobRTC for anonymity.

Under the crowdsourcing aspect, mostly, the forum feature of BobRTC was mentioned. For instance, B1 says he shares his knowledge with other users in the comments, but he is also getting creative ideas on what to do next. He also helps out other people with translating their call recordings of the scammers. B4 and B5 mention the IRC chat to be able to communicate with other users to share inside information, although B5 adds that the IRC chat has been mostly inactive when he used it. Another crowdsourcing aspect is the number sourcing: B5 describes that the phone numbers on BobRTC are partly crowdsourced using RoboKiller's service, which crowdsources its numbers from the devices of the users. Also, scammer numbers of PopupDB.org, where users add their found pop-us, get imported into the phonebook. B3 explains that BobRTC has some costs involved to be able to run the service, from phone bills to hosting provider costs. In the beginning, the developers paid for everything, but now there has been a donation scheme set up which, with a total of over 33,000 users, manages to pay for the costs at this time. B2 is donating for the service as he understands that the service needs to be supported to be able to continue to run. B3 adds that the moderator team is also monitoring the number being added to make sure that they are indeed scammer numbers. Also, it was stated by B3 that using crowdsourcing, not only one person is calling a number all day but thousands of people.

This also leads to the perceived impact: it is B3's opinion that because of thousands of people calling scammers all day that this has an impact on them. B4 made the experience that scambaiting scammers demotivated them so much that they would scream at real customers and that he had scammers telling him that they have had no sales all day. B1 states that while each scambaiter has different methods of scambaiting, in the end it takes up the scammer's resources. He emphasized that he reported a United States-based "money mule" to the authorities and they took action. B5 recalls the investigation by popular YouTubers Jim Browning and Karl Rock, which lead to the arrests of the masterminds of a particular scam call center. As a side effect, these videos also raise awareness as more people will know about the scam, which results in fewer victims. He also states that he has been reporting websites belonging to scammers to the respective hosting provider along with

evidence, and they have taken it down. Now, it is interesting to see the perspective of the scammers, which was coded as an “actual impact”. S1 states that they all have experienced prank callers daily. She says that the use of abusive language by the scambaiters affects her, and it disturbs the work she is doing. Although she claims the impact is not so high, it is still annoying. She blocks the scambaiters’ numbers however she also realized that they find another way of calling again. S2 did not experience many scambaiters: she just received one prank call in the six months she was working in the scam call center. However, that one prank call resulted in her getting fired as the scambaiter had her personal details which caused the call center to be scared of getting tracked down. She also states that usually, scambaiting calls are not a threat as they are just prank calls. As a counter measure, they are shutting down their inbound number every two or three days so that scambaiters would have to search for the new number. S3 says he has received a lot of these calls, which caused the call center to temporarily shut down their inbound number for some time until the calls stopped. S4 explains that the scambaiting calls and activities had a huge impact and decreased the daily turnover from around $100,000 to $55,000 and even less since all they would get was prank calls all day. He also says that in terms of reporting the scam call centers it is a “tug of war”: scambaiters and legitimate organizations such as Microsoft on one side, the call center on the other side. Whichever one is more influential the authorities will side with them. It is about the pressure. If it is high enough, the scam call center can be taken down.

Figure 4-1: Word cloud scambaiter interviews

Figure 4-2: Word cloud scammer interviews

5 Discussion

To answer the research question it has to be verified if the obtained answers are matching the question. As requirement, it needs to be checked if BobRTC is indeed a crowdsourcing tool. The interview partners explained how the numbers are being added to the system, which relies on the users to search for scammer numbers and to add them. This would fit the definition explained in the theoretical background section of the thesis: microworking & tasks. Another source of numbers is the RoboKiller app which itself crowdsources its numbers from user devices. As quoted before already, “A bogeyman is always the best connecting link” (Pelzer et al., 2012, p. 66). This is true here as well for the motivation of the users which is partially to fight the scammers together and additionally they see it as a fun activity that also matches the crowdsourcing characteristics (Pelzer et al., 2012, p. 48). To create fun, gamification elements can be used (Pelzer et al., 2012, p. 80). This is the case with BobRTC which awards XP points for every minute the user has spent on a call with the scammers. These XP points can unlock certain features and are used as a status to compare to other users. It was stated though that the use of XP on BobRTC is a little unclear and does not provide that many additional features. Other ways of creating fun for the users are the voice bots, which can talk to the scammer automatically and create funny conversations based on the voice bot which is engaged, and simply the possibility to call scammers and prank with them. Another way that BobRTC acts as crowdsourcing platform is the possibility to share information on the BobRTC forum and on each scammer number. It is a feature that many scambaiters require to be able to collaborate and BobRTC provides such features according to the interviewees. In the theoretical part it was already explained that crowdfunding as part of crowdsourcing has four sub-categories: donation-based, reward-based, equity-based, and peer-to-peer lending. BobRTC is falling into the donation-based crowdfunding category as the user is donating a specific amount of money but receives intangible benefits in return on the platform, such as a donor badge on the user profile. Obviously, the donors are part of the BobRTC community and are users of the same platform. So it can be concluded BobRTC is indeed a crowdsourcing platform.

An important reason why scambaiters are using this platform, in particular, is the security/privacy concern. Many scambaiters state that BobRTC protects their identity from scammers by not requiring real information to sign up for the service as well as

hiding the identity from the scammers by using a fake caller ID, which also changes on each call, making it impossible for the scammers to trace the scambaiters.

The influence BobRTC and its users have on the scam call centers variates on who is being asked. While all interviewed scambaiters think that their work has definitely some impact, some of the individuals out of the scammer group did not experience that much impact on their work by the calls and other scambaiting activities. Other scammer individuals said it definitely has an impact, and they temporarily shut down the inbound numbers to avoid receiving the calls. The amount of calls irritates the agents, which S1 confirmed and it prevents them from taking real victim calls. The biggest impact was reported by S4, who explained a massive decrease in revenue for the day. While there is no evidence that this has been caused by BobRTC in this instance, generally speaking BobRTC provides a tool with this possible effect since the caller ID changes on every call, making it impossible to block the calls coming from BobRTC. For this impact it requires a lot of users or calls focused on one particular call center as S4 explained that they received many calls which caused this loss in revenue. This can also be achieved through BobRTC's Auto-Redial feature as the interviewed scambaiters stated it reduces the time needed to make another call, and it adds convenience. Another way of having an impact on scammers is by collecting information, researching, and submitting it to various actors such as involved companies. As explained above, BobRTC provides a platform for scambaiters to collaborate and work together to research. This also has an impact, as proven by B5, who successfully reported websites used by scammers to the hosting companies and managed to shut them down. Another feature of BobRTC, which was not mentioned during the interviews, is that the platform displays the VoIP provider of each scammer phone number, which makes it easy to identify who to contact in order to get the phone number taken down.

Scambaiting requires a certain mass of scambaiters to have an impact on scam call centers with different methods as explained above. In order to have it work over a longer period of time, either the same people constantly do scambaiting or new people join the community constantly to replace those who retire from scambaiting. BobRTC uses gamification elements to keep users active and to attract new users to it so that mass is being achieved. Also, to achieve this impact, multiple scambaiters have to work together. This is only possible through platforms such as BobRTC as

only those provide a platform for scambaiters to unite and to focus on a specific number, gather information, and call them over and over again.

6 Conclusion

6.1 Limitations

Three limitations can be identified. The first limitation is the subjectivity of qualitative research since the process is not subject to intersubjective verification (Lamnek, 2010, p. 89). Also, even though a standardized process was used, the content analysis does not always work in the same manner: it has to be adapted to the specific material and situation (Mayring, 2015, p. 51). Mayring also requires the content analysis to be embedded in the communication context (Mayring, 2015, p. 50). However, this is a subjective decision. Different choices could be made. The same applies for the creation of the category system: Mayring states that in standard literature for content analysis, there is little to no guidelines or help (Mayring, 2015, p. 51). This means that the categories could be different with another researcher. For the findings, the subjectivity of the different steps means the results could vary from researcher to researcher. To somewhat offset that problem, the methodology is explained in detail.

The second limitation of this thesis might be the sample size of the study, the number of expert interviewees. Gläster & Laudel state that the number of interviews results from the distribution of information among the actors and from the requirements of empirical validation (Gläser & Laudel, 2010, p. 104). Especially regarding the empirical validation, the methodology does not prescribe a specific amount of interviews - it is rather a matter of discretion (Gläser & Laudel, 2010, p. 104). They state that there is no final answer to this question, but the more interviews were conducted, the higher the empirical validity is (Gläser & Laudel, 2010, p. 104). Most of the time, expert interviews are not the only data collection method. They will be supported by literature analysis, which will add additional observations (Gläser & Laudel, 2010, p. 105). The combination of multiple data collection methods is called triangulation (Gläser & Laudel, 2010, p. 105). In terms of the distribution of the information among the actors, the amount of interviews is very limited, especially the group of scammers. While Gläser & Laudel state that it might be sufficient to interview three or four central actors, this might be true for the scambaiter group as they are usually connected with each other, and it seemed the information collected was mostly congruent (Gläser & Laudel, 2010, p. 104). For the other group, the

scammers, this is more complicated as there are so many different scam call centers, and not all might have been experiencing scambaiting calls. The variation of information and opinions was variating a lot, hinting that not all the available information has been captured. The difficulty is to find enough interview partners who are or were working in such scam call centers who are willing to come forward and share their information on a recorded call. Some of the interview partners had to be persuaded and promised that their names will not be shared, due to privacy concerns. Interestingly, when trying to recruit interview partners, even some scambaiters declined to have the interview for these reasons even though they do not break the law in contrary to the scammers.

The third limitation might be the truthfulness and objectivity of the statements of the interviewees. In daily life, people are more often exposed to truthful statements than to deceptive statements. This rarity of deceptive statements makes people assume that honest statements are the most likely to occur, and they, therefore, have the tendency to judge others as being truthful (Vrij & Baxter, 2000, p. 26). Statements that sound plausible and contain many details will also be considered to be true (Vrij & Baxter, 2000, p. 26f). This is called “truth bias” (Vrij & Baxter, 2000, p. 26). Researchers found that nonverbal behavior is harder to control when lying than speech content (DePaulo and Kirkendol, 1989; Ekman, 1992; Ekman and Friesen, 1974; Vrij, 2000). That is why observers can and will primarily rely upon the nonverbal gestures to judge the veracity of statements, a hypothesis which was confirmed by Vrij & Baxter in an experiment (Vrij & Baxter, 2000, pp. 27, 34). The interviews in this thesis were conducted via voice call; it was not possible to observe non-verbal cues that may indicate the subject was lying (Opdenakker, 2006, p. 5). A group of scammers could have an interest in lying about specific topics to avoid negative consequences to their job or may have been trained to respond to questions about their employment to disguise the criminal nature of their job. The group of scambaiters does not have such a big interest in lying, however, as users and supporters of the BobRTC platform, there might be a tendency to be less objective and rather praise than criticize the platform. To counter this, it was made clear to participants of both groups during the briefing for the interview that the truth is important as the research tries to capture the most realistic image of the situation.

6.2 Future research topics

A problem mentioned by many interviewed scambaiters is the lack of cooperation with the affected companies and law enforcement agencies. As already explained in the theoretical background, law enforcement agencies currently see some problems with the perceived information quality as well as legal liabilities regarding civilian involvement (Huey et al., 2013, p. 94f). Also from a legal point of view, scambaiters cannot file police complaints as they have not been victimized by a (cyber) crime. This poses a problem because the submitted information would not be used. It should be researched how more effective relations between scambaiters and other players as mentioned above could be achieved (Huey et al., 2013, p. 95). On the scambaiter side, this could be a set of rules which information is required, how to structure and organize the information in a way that the other parties are content with the quality. On the other side, be it corporations or law enforcement agencies, there should be a process that is designed to allow informants such as scambaiters to provide information that could be verified and also leads to investigations. For this to happen, depending on the legal system of each country and state, it might be required to adapt the legislation.

Another topic might be the categorization of scambaiters. As explained in the theoretical background, Zingerle & Kronman identified and categorized seven types of scambaiters for the Nigerian 419 email scam, based on their activities, techniques, legality aspect, and motivation (Zingerle & Kronman, 2013, p. 353ff). These types of scambaiters are very specific for the Nigerian 419 email scam and do not match with scambaiters targeting telephone scams such as IRS/SSA or tech support scams. For instance, the type “The Safari Agents” does not exist here as the telephone scammers do not travel to different places to collect money. Telephone scammers work from call centers or from home as freelancers, and they receive the payments mostly using MoneyGram, Western Union, through gift cards or credit cards (Miramirkhani et al., 2017, pp. 2, 11; Tabron, 2016, p. 46; Tzani-Pepelasi et al., 2020, pp. 163, 168; US Department of Justice, 2020b, pp. 5, 8). There is no need for them to travel. Another type that does not exist at all with telephone-based scams is “The Romance Scam Seeker”. It can be concluded that the types are too specific to email-based scams and do not fit telephone-based scams. It would be a future research topic to create types of scambaiters for telephone-based scams based on the activities, ethical and legal

boundaries, and motivation of the scambaiters. On the scammer.info forum, a user already proceeded to categorize scambaiters into five levels based on their activities (Scammer.info, 2020a). Although the methodology might not follow scientific criteria, for instance, it is not clear where the person derived the data from or which data set or data collection was being used, this categorization is a very interesting beginning for new research.

6.3 Summary

The motivations of the users for scambaiting ranges from trying to shut down scammers to just fun and is being supported by BobRTC's features such as voice bots, Auto-Redial, and more. The scambaiters' activities are diverse and are using various methods to achieve their goal. Another way BobRTC as a crowdsourcing platform helps is by adding convenience in finding scammer numbers to call and by protecting its users' privacy by using different caller IDs for every call. Crowdsourcing methods can have huge impacts on the operations of scam call centers, depending on the strategy chosen by the users and the concentration of efforts on one particular target. This was confirmed by the interviewed scammers. This impact is just possible through the use of crowdsourcing platforms such as BobRTC as they provide means to communicate and collaborate with other scambaiters and to focus on specific call centers of their choice.

References

BBC Panorama. (2020). Scam call centre owner in custody after BBC investigation. Retrieved October 16, 2020, from https://www.bbc.com/news/technology-51740214

Bidgoli, M., & Grossklags, J. (2017). "Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing. *ECrime Researchers Summit, ECrime*, 57–69. https://doi.org/10.1109/ECRIME.2017.7945055

Button, M., Lewis, C., & Tapley, J. (2008). *Fraud typologies and victims of fraud*. Portsmouth. Retrieved from https://researchportal.port.ac.uk/portal/files/1926122/NFA_report3_16.12.09.pdfButton,

Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation and Governance*, *12*(1), 101–114. https://doi.org/10.1111/rego.12125

Clancy, D., Williams, G., Kubis-, B., Sullivan, S., Sullivan, S., & Gillett, A. (2020). Operation LINDEN - Unsolicited Marketing Communications Strategy Meeting (pp. 1–9). London: ICO. Retrieved from https://ico.org.uk/media/action-weve-taken/2617862/operation-linden-20200204.pdf

Deutsche Gesellschaft für Soziologie, & Berufsverband Deutscher Soziologinnen und Soziologen. (2017). Ethik-Kodex. *Forschung*, 2–5. Retrieved from http://www.soziologie.de/de/die-dgs/ethik-kodex.html

Discommunications LLC. (2020). BobRTC. Retrieved October 17, 2020, from https://bobrtc.tel/

Dushnitsky, G., & Marom, D. (2013). Crowd Monogamy. *Business Strategy Review*, (4), 24–26. https://doi.org/10.1111/j.1467-8616.2013.00990.x

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, *50*(1), 25–32. https://doi.org/10.5465/AMJ.2007.24160888

Elliot, R. (2016). Couple says IRS scammer called SWAT on them. Retrieved August 6, 2020, from https://www.wsbtv.com/news/local/cherokee-

county/couple-says-irs-scammer-called-swat-on-them/407362161/

FCC. (2019). Combating Spoofed Robocalls with Caller ID Authentication. Retrieved October 14, 2020, from https://www.fcc.gov/call-authentication

Federal Bureau of Investigation. (2019). 2019 Internet Crime Report. *Federal Bureau of Investigation - Internet Crime Complaint Center*, 1–28. Retrieved from https://pdf.ic3.gov/2019_IC3Report.pdf

Federal Communications Commission. (2019). *FCC Issues Report On Illegal Robocalls | Federal Communications Commission*. Retrieved from https://www.fcc.gov/document/fcc-issues-report-illegal-robocalls

First Orion. (2018). *Nearly 50% of U.S. Mobile Traffic Will Be Scam Calls by 2019*. Los Angeles. Retrieved from https://firstorion.com/nearly-50-of-u-s-mobile-traffic-will-be-scam-calls-by-2019/

First Orion. (2019). *Scam Call Trends and Projections Report - Summer 2019*. Retrieved from http://firstorion.com/wp-content/uploads/2019/07/First-Orion-Scam-Trends-Report_Summer-2019.pdf

FTC. (2019). FTC Releases FY 2019 National Do Not Call Registry Data Book. Retrieved July 8, 2020, from https://www.ftc.gov/news-events/press-releases/2019/10/ftc-releases-fy-2019-national-do-not-call-registry-data-book

FTC. (2020). FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against ‘ Routing and Transmitting ’ Illegal Coronavirus- related Robocalls. Retrieved July 8, 2020, from https://www.ftc.gov/news-events/press-releases/2020/05/ftc-fcc-send-joint-letters-additional-voip-providers-warning

Gläser, J., & Laudel, G. (2010). *Experteninterviews und qualitative Inhaltsanalyse* (4. Auflage). Wiesbaden: VS Verlag für Sozialwissenschaften.

Google Inc. (2020). Google Play Store: RoboKiller - Spam and Robocall Blocker. Retrieved October 13, 2020, from https://play.google.com/store/apps/details?id=com.robokiller.app

Gupta, P., Srinivasan, B., Balasubramaniyan, V., & Ahamad, M. (2015). Phoneypot: Data-driven Understanding of Telephony Threats, (February), 8–11. https://doi.org/10.14722/ndss.2015.23176

Gustafsson, J. (2017). *Single case studies vs. multiple case studies: A comparative study*. *Academy of Business, Engineering and Science Halmstad University, Sweden*. Halmstad University. https://doi.org/January 12, 2017

Harley, D., Grooten, M., Burn, S., & Johnston, C. (2012). My Pc Has 32 , 539 Errors : How Telephone Support Scams Really Work, (September), 1–8.

Helfferich, C. (2005). *Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Huey, L., Nhan, J., & Broll, R. (2013). "Uppity civilians" and "cyber-vigilantes": The role of the general public in policing cyber-crime. *Criminology and Criminal Justice*, *13*(1), 81–97. https://doi.org/10.1177/1748895812448086

Javid, M. Bin, & Chakraborty, S. (2019). A Call to Deal with Technical Support Scams. *International Journal of Research in Engineering, Science and Management*, *2*(4), 406–410. Retrieved from https://www.ijresm.com/Vol.2_2019/Vol2_Iss4_April19/IJRESM_V2_I4_113.pdf

Lamnek, S. (2010). *Qualitative Sozialforschung* (5., überar). Weinheim: Beltz Verlag.

MAXQDA. (2020). MAXQDA. Retrieved October 20, 2020, from https://www.maxqda.de/software-inhaltsanalyse

Mayring, P. (2015). *Qualitative Inhaltsanalyse - Grundlagen und Techniken* (12., übera). Weinheim: Beltz Verlag.

Merriam, S. B. (2009). *Qualitative Research: A guide to implementation* (3rd Editio). San Francisco: Jossey-Bass.

Microsoft Digital Crimes Unit. (2018). Online scammers cost time and money. Here's how to fight back. Retrieved July 12, 2020, from https://news.microsoft.com/on-the-issues/2018/10/15/online-scammers-cost-time-and-money-heres-how-to-fight-back/

Miramirkhani, N., Starov, O., & Nikiforakis, N. (2017). Dial One for Scam: A Large-Scale Analysis of Technical Support Scams, (March). https://doi.org/10.14722/ndss.2017.23163

Mollenhauer, K., & Rittelmeyer, C. (1977). *Grundfragen der Erziehungswissenschaft* (1. Edition). München: Juventa-Verlag.

Mubarak, M. F., Yahya, S., & Shaazi, A. F. A. (2019). A Review of Phone Scam Activities in Malaysia. In *IEEE 9th International Conference on System Engineering and Technology (ICSET)* (pp. 441–446). Malaysia.

Mustafa, H., Xu, W., Sadeghi, A. R., & Schulz, S. (2014). You can call but you can't hide: Detecting caller ID spoofing attacks. *Proceedings of the International Conference on Dependable Systems and Networks*, 168–179. https://doi.org/10.1109/DSN.2014.102

Nakamura, L. (2014). "I will do everything that am asked": Scambaiting, digital show-space, and the racial violence of social media. *Journal of Visual Culture*, *13*(3), 257–274. https://doi.org/10.1177/1470412914546845

Ofcom. (2019). *Nuisance calls and messages. Update to ICO-Ofcom joint action plan*. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0034/194974/nuisance-calls-joint-action-plan-2020.pdf

Opdenakker, R. (2006). Advantages and Disadvantages of Four Interview Techniques in Qualitative Research. *Qualitative Social Research*, *7*(4), 13. https://doi.org/10.17169/fqs-7.4.175

Pelzer, C., Wenzlaff, K., & Eisfeld-Reschke, J. (2012). *Crowdsourcing Report 2012 - Neue Digitale Arbeitswelten*. Berlin: epubli GmbH.

PopupDB. (2020). PopupDB. Retrieved October 19, 2020, from https://popupdb.org/popups/5f8c8020463ab

Rodríguez, P., Cerviño, J., Trajkovska, I., & Salvachúa, J. (2012). Advanced videoconferencing services based on WebRTC. In P. Kommers & N. Bessis (Eds.), *IADIS International Conferences, Web Based Communities and Social Medial 2012, Collaborative Technologies 2012* (pp. 180–184). Lisbon. Retrieved from https://www.researchgate.net/profile/Piet_Kommers/publication/323277996_WBC_CT_2012/links/5a8ba095aca272017e63ae0e/WBC-CT-2012.pdf#page=201

Scammer.info. (2020a). 5 Levels of Scambaiters. Retrieved October 21, 2020, from

https://www.scammer.info/d/40239-5-levels-of-scambaiters

Scammer.info. (2020b). Scammer.info. Retrieved October 17, 2020, from https://www.scammer.info/

Schall, D. (2012). *Service-Oriented Crowdsourcing - Architecture, Protocols and Algorithms*. Vienna: Springer. https://doi.org/10.1007/978-1-4614-5956-9

Shimomura, T., & Markoff, J. (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw - By the Man Who Did It*. New York: Hyperion.

Shover, N., Coffey, G. S., & Hobbs, D. (2003). Crime on the Line: Telemarketing and the Changing Nature of Professional Crime. *British Journal of Criminology*, *43*(3), 489–505. https://doi.org/10.1093/bjc/43.3.489

Sredojev, B., Samardzija, D., & Posarac, D. (2015). WebRTC technology overview and signaling solution design and implementation. *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015 - Proceedings*, (May), 1006–1009. https://doi.org/10.1109/MIPRO.2015.7160422

Srinivasan, B., Kountouras, A., Miramirkhani, N., Alam, M., Nikiforakis, N., Antonakakis, M., & Ahamad, M. (2018). Exposing search and advertisement abuse tactics and infrastructure of technical support scammers. *The Web Conference 2018 - Proceedings of the World Wide Web Conference, WWW 2018*, 319–328. https://doi.org/10.1145/3178876.3186098

Staatsanwaltschaft Osnabrück. (2016). Online-Betrug - Landeskriminalamt Niedersachsen und Staatsanwaltschaft Osnabrück durchsuchen erfolgreich in Indien. Retrieved August 8, 2020, from https://www.staatsanwaltschaft-osnabrueck.niedersachsen.de/startseite/aktuelles/presseinformationen/online-betrug---landeskriminalamt-niedersachsen-und-staatsanwaltschaft-os-nabrueck-durchsuchen-erfolgreich-in-indien-146597.html

Sukma, N., & Chokngamwong, R. (2018). Increasing the efficiency of One-time key Issuing for the First Verification Caller ID Spoofing Attacks. *Proceeding of 2018 15th International Joint Conference on Computer Science and Software Engineering, JCSSE 2018*, 1–6. https://doi.org/10.1109/JCSSE.2018.8457341

Tabron, J. L. (2016). *Creating Urgency in Tech Support Scam Telephone Conversations*. Hofstra University. Retrieved from https://search.proquest.com/openview/27248dfbc9c402f2f2ab2fa8d6c0adb0/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y

Teltech Systems Inc. (2020). RoboKiller.com. Retrieved October 13, 2020, from https://www.robokiller.com/

Transparency International. (2019). *Corruption Perceptions Index*. Retrieved from https://www.transparency.org/en/countries/india

Tu, H., Doupe, A., Zhao, Z., & Ahn, G. J. (2016). SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam. In *2016 IEEE Symposium on Security and Privacy, SP 2016* (pp. 320–338). IEEE. https://doi.org/10.1109/SP.2016.27

Tucci, C. L., Afuah, A., & Viscusi, G. (2018). *Creating and Capturing Value through Crowdsourcing* (First Edit). Oxford: Oxford University Press.

Tzani-Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R., & Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting*, *12*(1), 163–178. Retrieved from http://web.nacva.com/JFIA/Issues/JFIA-2020-No1-10.pdf

US Census Bureau. (2019). *Census Bureau Projects U.S. and World Populations on New Year's Day*. *US Census Bureau*. Retrieved from https://www.census.gov/newsroom/press-releases/2019/new-years-population.html

US Congress. (2009). Truth in Caller ID Act of 2009. Retrieved October 25, 2020, from https://www.congress.gov/111/plaws/publ331/PLAW-111publ331.pdf

US Department of Justice. (2020a). Justice Department And Indian Authorities Announce Enforcement Actions Against Technical-Support Fraud Scheme Targeting Seniors. Retrieved October 17, 2020, from https://www.justice.gov/opa/pr/justice-department-and-indian-authorities-announce-enforcement-actions-against-technical

US Department of Justice. (2020b). United States v. Kahen. New York: US

Department of Justice. Retrieved from https://www.justice.gov/opa/press-release/file/1240031/download

US Department of Justice. (2020c). United States v. Palumbo. New York: US Department of Justice. Retrieved from https://www.justice.gov/opa/press-release/file/1240026/download

Vanhaverbeke, W., Vermeersch, I., & De Zutter, S. (2012). Open innovation in SMEs: How can small companies and start-ups benefit from open innovation strategies? *Information Management*, (March), 1–99. https://doi.org/10.1108/13552551211239492

Vrij, A., & Baxter, M. (2000). Truth and Lies in Elaborations and Denials. *Expert Evidence*, *7*(1), 25–36. Retrieved from http://proxy.library.brocku.ca/login?url=http://search.proquest.com/docview/619825021?accountid=9744

Wall, D. S., & Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology and Criminal Justice*, *7*(4), 391–415. https://doi.org/10.1177/1748895807082064

Yin, R. K. (2003). *Case study research: Design and methods* (3rd Editio). Los Angeles: Sage Thousand Oaks.

Zingerle, A., & Kronman, L. (2013). Humiliating entertainment or social activism? Analyzing scambaiting strategies against online advance fee fraud. *Proceedings - 2013 International Conference on Cyberworlds, CW 2013*, (September 2012), 352–355. https://doi.org/10.1109/CW.2013.49

Appendix

Questionnaire - Scambaiter

Hi,

Thanks for participating and helping me out with the interview! Before we start I just want to introduce myself. As you probably know I'm NeeP, the scambaiter and this interview is for my bachelor thesis. The title is "Application of crowdsourcing platforms for fighting telephone scams" and I want to research if and how crowdsourcing platforms such as BobRTC can contribute to obstruct the activities of the scammers. The interview will take about 30 minutes. I will ask you questions regarding your experience with this platform and about your own scambaiting background and experiences. Please try to answer as honest as possible, don't exaggerate or bend the truth, I'm not judging you on the things you say. The main focus is to capture the reality and to get the most accurate picture of the situation as possible. I will anonymize potentially identifiable information later on. The interview will be recorded from my side and later transcribed to text which I will further analyze and summarize for the thesis. The recordings will not be shared however the transcripts will be submitted to my supervisor and professor. Direct quotes might appear in the thesis.

1. What is your personal background? Education? Age? Team?
2. What do you define as scambaiting? What is scambaiting for you?
3. Are there different groups of scambaiters?
4. How did you start scambaiting?
5. Since how long have you been scambaiting?
6. What is your motivation?
7. Do your friends scambait?
8. (Do you earn money with scambaiting? Do you pay money for scambaiting? Donations?)
9. Do you get recognition out of scambaiting?
10. How long do you scambait at a time? How much in a week/month?
11. Which priority does scambaiting have compared to other leisure activities?
12. Which measures are you taking? Reporting to police/companies? Warning victims? Publishing information?

13. Do you report scammers to police or companies such as Microsoft or the hosts?
14. **Do you think collaborating with other users is beneficial? How so?**
15. **Which tools are you using? How do you find numbers, how do you call?**
16. **Do you use BobRTC?**
17. **(How does it work? Who is contributing? Who is using them?)**
18. **How is it funded?**
19. **Tell me how your typical use of BobRTC looks like, which steps you take etc.**
20. **What sets it apart from other, more conventional VoIP platforms like Skype?**
21. **Which feature(s) do you like the most?**
22. **How are the numbers added to the phonebook? (Integration with**
23. **How do you think the Voice Bots/Dial Buddies are having an impact?**
24. **Do you think the Auto-Redial/Assistance Dial helps you in speeding up the process of scambaiting?**
25. **What effect does your work have? Success/failure stories?**
26. **Has BobRTC helped you at that time in any way?**
27. **Do you have contact with other scambaiters? How intense? How are you connected?**
28. **How is BobRTC helping you to collaborate with others?**
29. **Does it integrate with other scambaiting platforms?**
30. Are you scared to face any backlash from the scammers?
31. **What measures are you taking to protect yourself from scammers? Is BobRTC of any help?**
32. **How does BobRTC keep users active? Is there anything that keeps scambaiting with BobRTC interesting?**
33. **What would you improve?**
34. **Do you think scambaiting has any effect on scammers?**
35. **Do you know of any factual effects?**
36. Should the government or affected companies support scambaiting?
37. What can be improved – among scambaiters / collaboration between scambaiters and authorities & companies?
38. What should the authorities do to fight scams?
39. How do the companies (web hosting providers, phone providers of the scammers, Microsoft) react when reporting scams to them? Positive feedback? Unwilling to process the information?

Questionnaire - Scammer

Hi,

Thanks for participating and helping me out with the interview! Before we start I just want to introduce myself. As you probably know I'm NeeP, the scambaiter and this interview is for my bachelor thesis. The title is "Application of crowdsourcing platforms for fighting telephone scams" and I want to research if and how crowdsourcing platforms such as BobRTC can contribute to obstruct the activities of the scam call centers. The interview will take about 30 minutes. I will ask you questions regarding your experience with prank callers and about your own background and experiences as tech support agent. Please try to answer as honest as possible, don't exaggerate or bend the truth, I'm not judging you on the things you say. The main focus is to capture the reality and to get the most accurate picture of the situation as possible. I will anonymize potentially identifiable information later on. The interview will be recorded from my side and later transcribed to text which I will further analyze and summarize for the thesis. The recordings will not be shared however the transcripts will be submitted to my supervisor and professor. Direct quotes might appear in the thesis.

1. What is your personal background? Education? Age?
2. Since how long have you been working there?
3. How did you start working in this industry?
4. What is your motivation?
5. Do your friends work in the same industry?
6. How is the salary compared to legitimate call centers?
7. Which type of call center process do you work in?
8. Which country/language are you targeting?
9. Are prank callers a problem?
10. **How often do you receive prank calls per day?**
11. **How did it evolve over time, over the course of the last years?**
12. **What do you think of prank callers? Are they just an annoyance or a real threat?**
13. **Do you think the prank callers are individuals or an organized group?**
14. **Do you think prank callers are having a bigger impact if they are calling as group/in bulk or individually?**

15. **What exactly do prank callers do? Can you guide me through the experience?**
16. **Have you received a call with an automated voice talking instead of a real human?**
17. **Do you sometimes receive calls from the same prank caller over and over?**
18. **What do you do when you receive prank calls?**
19. Has there been any special prank caller that you remember?
20. **Do you recognize different groups/types of prank callers?**
21. **What is the effect of prank calls on your work flow?**
22. **What is the effect on the call center? Do the managers change their workflow temporarily or permanently?**
23. **Are there any measures you are taking to avoid prank callers?**
24. **Can you block prank caller numbers?**
25. Have you received any targeted attack?
26. **Have you seen any information about your call center being posted online? Videos? Forum posts?**
27. **Is your management worried about these things happening?**
28. (Have you had to change your call center number?)
29. **Do you report prank callers to your colleagues or other centers?**
30. **Do you take actions against prank callers? Trying to find out who they are?**
31. **What do you think their motivation is?**
32. How strict does the government/police take action against centers?

Declaration of Academic Integrity

I hereby certify that I have prepared this thesis independently and without the use of any auxiliary materials other than those indicated. All passages taken verbatim or in spirit from published and unpublished writings are identified as such. The work has not been submitted in the same form to any other examining authority.