THE DEVELOPMENT OF VISHING FRAUD DURING THE COVID PANDEMIC

ELLEN BERGLUND MOLIN

Wordcount: 8835

Degree Project in Criminology
30 Credits Master's Programme (Two-Year)
June 2021

Malmö University
Faculty of Health and Society
205 06 Malmö

THE DEVELOPMENT OF VISHING FRAUD DURING THE COVID PANDEMIC

ELLEN BERGLUND MOLIN

Berglund Molin, E. The development of vishing fraud during the covid pandemic. *Degree project in Criminology 30 Credits.* Malmö University: Faculty of Health and Society, Department of Criminology, 2021.

The number of fraud crimes has increased significantly over the past decade. The primary reason for this is the extensive and increasing use of the internet, as well as technical developments. In 2020, frauds through social manipulation such as vishing fraud were increasingly prominent. Due to the COVID-19 that marked the year, the study intends to study how vishing fraud has been affected by the pandemic in Sweden, and what other factors that could explain the increase in fraud modes through social manipulation such as vishing? Further the study also examines if the current situation affected or influenced future working methods or created new insights for the parties concerned. An analysis of the examined material showed that the pandemic has to some extent had an impact on vishing fraud, such as which authorities the fraudsters claim to come from. It has also been seen for home visits where several have been corona related. However, it is considered too early to be able to draw conclusion on the exact impact that the pandemic has had on vishing fraud and/or crime, hence such studies may be performed after the pandemic subsided. Furthermore, all parties emphasized the importance of continued cooperation in order to be able to work more effectively both for investigation purposes and for crime prevention purposes.

Keywords: COVID-19, financial crime, fraud, human psychology, social engineering, vishing attacks.

FOREWORD

I would like to extend a big thank you to those who have chosen to participate in this study, without whom the study could not have been carried out. Furthermore, I would like to thank my supervisor Juliana Holeksa for all the advice and support she has given me during the work. Her advice has been invaluable in the final stage of the study.

TABLE OF CONTENTS

1 INTRODUCTION

In 2019, Sweden participated in the international initiative First Light, coordinated by Interpol, as a global effort primarily against fraud and money laundering. The initiative was based on the extensive problems that financial crime entails, both globally and nationally. As a result of the operation that lasted from September to November 2019, Swedish police seized 20 million SEK and according to Interpol 1.3 billion SEK was seized in total (Polisen, 2020c). Over the last 30 years, financial crime has intensified and become an increasingly problematic issue (International Compliance Association, 2020). In addition, financial crime is exceedingly costly, said to be a trillion-dollar industry globally (Hasham, Joshi, & Mikkelsen, 2019). Apart from the economic aspect, financial crime is also socio-economically costly since it has a major detrimental impact on society, partly by its effect on the welfare of the state and partly by threatening global security in several ways (Handels, 2018). Financial crime is a complex area that covers innumerable approaches to acquire money illicitly. It ranges from minor fraud offences to complex large-scale operations linked to organized crime, not limited by national borders (Interpol, 2021). Due to globalization, developing technology and the change in social relations, financial crime is forced to adapt to these conditions. This means that the methods used by criminals are constantly improving, becoming more complex and comprehensive in order to deceive their victims.

Over the past decade there has been a significant increase in fraud offences, where an increase of 89% has been noted (Brå, 2020). This has several explanatory factors, primarily the extensive and increasing use of the internet, and the rapid technological development which enables the development of new methods and approaches for committing fraud (ibid). Due to unimaginable possibilities for both communication and consumption and with increased opportunities to use technical tools, such as being able to identify oneself with electronic identification (e-ID), more complex and comprehensive procedures and methods to exploit weaknesses in the systems and commit fraud have evolved (Brå, 2020a; Polisen, 2016). In 2018, frauds that were linked to the use of the internet accounted for two-thirds of all reported frauds in Sweden (Brå, 2020). In 2020, 218 000 fraud crimes were reported, which signifies a decrease of 11% compared to the previous year (Brå, 2020a). The reason for the overall decrease of frauds consists of a largely reduced number of card frauds (a reduction by 25%), which otherwise is the most common fraud reported (Säkerhetskollen, 2020a). One of the reasons for the declining statistics for card fraud is a possible effect of the new EU directive, PSD2 (Payment Services Directive 2), which improves the terms for safer card payments since it includes stronger authentication and identification for card payments in order to reduce fraud (Svensk Handel, 2020).

In 2020, an increase was noted in the number of reports where elderly was exposed to fraud through voice calls, defined as vishing fraud (Polisen, 2020f). Fraud through social manipulation (social engineering) was thus the fraud mode that increased the most in 2020 (23%), where vishing fraud accounted for the largest increase (Brå, 2020a; Sveriges Radio, 2021, 18:10). In November, more than 700 reports of vishing fraud had been reported, with 80% of the victims being 70 years or older (Polisen, 2020f). On average, vishing fraud causes losses of approximately 10 million SEK every month, however, in November 2020, the

fraudsters had extracted approximately 24.5 million SEK in vishing fraud alone (Sveriges Radio, 2021, 10:40).

A significant increase for vishing fraud was first noted in 2018, where Nationella operativa avdelningen, Noa (National Operations Department), in response to this initiated a special national effort (Operation Dimma) with the aim of reversing the negative development and hence put an end to vishing fraud (Sveriges Radio, 2019). Vishing (voice phishing attack) is derived from a composition of the term's "voice" and "phishing". The Modus operandi (MO), the approach to vishing fraud, is where the fraudster, through the use of voice calls and social manipulation, deceives the victim into disclosing confidential, financial, or personal information, in order to provide for own financial gain (Polisen, 2020a).

2020 was affected by COVID-19 (coronavirus disease 2019, SARS-CoV-2) which has had a major impact both nationally and globally, and like other societal crises, the pandemic has been exploited by fraudsters in several different ways. By taking advantage of the situation caused by the coronavirus and the occurrences of adverse events as a result of it, several vishing frauds are considered to be corona related (Polisen, 2020).

1.1 Aim

The following study aims to analyze and examine the recent increase in vishing fraud in Sweden, specifically focusing on how vishing fraud has been affected by the COVID-19 pandemic in Sweden, and how the pandemic possibly is an explanatory reason for this increase. This will be achieved by primarily focusing on answering the following research questions:

1. How has vishing fraud been affected by the COVID pandemic?

2. What other factors can explain the increase in fraud modes through social manipulation such as vishing fraud?

3. Has the current situation affected or influenced future working methods or created new insights for the parties concerned?

2 THEORY AND PREVIOUS RESEARCH

2.1 Vishing fraud

Vishing refers to fraud that imply the use of voice calls, where the fraudster's MO is through social manipulation to deceive victims in order to obtain financial gain (Säkerhetskollen, 2020). By exploiting positions of trust or claiming to possess powers, the fraudster deceives the victims to refrain from, or perform certain acts, such as sign logins, approve transactions or disclose other sensitive information such as bank codes (Polisen, 2020a; NE, 2021). The fraudster persuades and convinces the victim to act in accordance with their given instructions (Krombholz et al, 2014). To achieve such procedures, they inspire great confidence and often act professionally in the social interaction, the fraudsters know exactly how to express themselves and what to emphasize in order to get the victim to comply with the instructions (Polisen, 2019).

The approaches used by fraudsters tend to vary, however, the fraudster often claims that something is urgent in order to cause stress to the victim. When being exposed to stressful situations or events, individuals are more inclined to make decisions that are less thought through (Säkerhetskollen, 2020). The fraudsters then try to establish some trust by assuring the victim that the situation will be resolved if they follow the instructions provided (ibid). Fraudsters often state that they are calling from authorities such as the police, hospitals, the public health authority, or financial institutions such as banks or loan companies, (referred to as authority fraud) meaning that they exploit the trust the general public has in such authorities, which increases the chances of the fraud to succeed, as individuals automatically tend to comply with authority figures (Brå, 2020; Zuoguang et al, 2021). In general, Swedish authorities and institutions insinuate reliability and low risk (Kantar Sifo, 2020). In 2020, the public health authority was one of the authorities in Sweden with the highest reputation (ibid). Since the influence of authorities is powerful, individuals tend to trust and adhere to what the fraudsters say without them needing to explain in further detail, meaning that in social engineering attacks (e.g., vishing fraud), authority is used as a very strong motivator (Hadnagy, 2018). Furthermore, several modern tools and techniques are often used in vishing frauds by the fraudsters to deceive their victims. For example, the use of number spoofing, where the dialing number is changed to the authority's authentic number. This technical possibility is often something that the victims are not aware of, meaning that the attacks are more likely to succeed (Yeboah-Boateng & Amanor, 2014). Due to such technology and other means, social engineering attacks are common globally (ibid). As described above, fraud through social manipulation (social engineering) was the fraud mode that increased the most in 2020 (Brå, 2020). Those primarily affected by such attacks are elderly, since there is a general perception that elderly lack or have less technical knowledge about how different technical means works, and therefore are less able to protect themselves against e.g., vishing fraud (Polisen, 2020b).

In Sweden, certain personal data are considered to be public documents, which means that the public can request e.g., social security numbers and other information through authorities such as the Swedish Tax Agency in accordance with offentlighetsprincipen, which is a part of the Swedish constitution law

(Regeringskansliet, 2014). Common in vishing fraud is that the fraudster prior to the fraud has acquired personal information about the victim, which increases the chances of the fraud succeeding since it makes the fraudster seem reliable and authentic (Polisen, 2020a). A further description of vishing fraud is referred to as home visits, which means that the fraudsters expand the possibilities of performing vishing attacks. In accordance with vishing fraud, the victims are misled by what they believe are trustworthy authorities into disclosing information when being confronted at their homes (Polisen, 2020e).

In the past, it was more common for fraudsters to engage exclusively in committing fraud offences. Today, however, it is more common for multi-criminal networks, who also engage in other criminal activities such as violent crime or drug related crimes, to engage in fraud. Fraud have become increasingly profitable and lucrative for criminals since the funds often are easily accessible (Säkerhetskollen, 2020c). These crimes are mainly committed by individuals and/or groups involved in organized crime, and in 2020 the police stated that specifically vishing fraud accounts for a large part of the criminal networks fundings (SVT, 2020). The structures and compositions of the frauds can be referred to as a pyramid or hierarchical organization, where one or more people on the top controls and organizes the procedures (ibid). For these people, the financial gain is often high, and the risks are considerably low (Operation Casino, 2021). Those on the top tier rarely commit the fraud themselves but rather use additional people included in their networks, these individuals tend to be young, and can be referred to as money launderers (SVT, 2020). They transfer funds that derive from fraud or other crimes through their bank account onto other accounts, and thus launder money originating from criminal activity (FBI, 2020). By using money launderers, those who control and manage the frauds can usually not be directly linked to the crime (Operation Casino, 2021). Because of this, vishing frauds often lead to money laundering offenses, since when investigating vishing frauds, linkages to money laundering are often detected (Polisen, 2020b). Furthermore, fraud can be in some instances defined as a serial crime, meaning that an individual perpetrator can commit several frauds on different occasions over a short period of time, and in combination with specific events (such as the COVID pandemic) which can enable a larger arena for fraud to be committed, extensive variations in the statistics can be seen from one year to another (Brå, 2020).

2.2 Social engineering

Social engineering attacks implicate extensive security threats globally (Zuoguang et al, 2021). With the continuous development of technical possibilities and new communication methods in combination with reduced personal interaction, the threat that social engineering entails is increasingly severe. Since the 1970s, social engineering attacks have expanded in popularity and in comparison, to traditional hackings and computer attacks, social engineers target individuals instead of targeting systems, meaning that they exploit weaknesses and vulnerabilities in human psychology. Social engineering can be referred to as an interdisciplinary field involving several aspects such as psychology, cognitive science, neuroscience, social psychology as well as computer science and cybersecurity (ibid). There are several different aspects of social engineering attacks: physical, social, socio-technical, and technical approaches (Krombholz et al, 2014). The

social approach is the most important aspect of a successful attack, where the basic premise is to manipulate the victims through persuasion. This can be done by for example pretending to be authority figures where they exploit the trust of authorities and induce curiosity in order to mislead and deceive the victims. The most common type of social attacks is those achieved through phone (vishing attacks). Further, socio-technical approaches include a combination between the social and the technical approach (this approach mostly occurs over the internet), where the attackers combine technical skills with social manipulation, this approach is the most efficient resource of social engineers. Further, the physical approach includes the attacker performing physical actions such as physical extortion to obtain sensitive, personal, or financial information (ibid).

Social engineering attacks occur due to the existence of three different factors: human vulnerabilities, effect mechanism and attack methods. Human vulnerabilities refer to psychological manipulation and social interaction that the social engineers attacker realize in order to deceive victims, or in some cases, that the attacker, through persuasion and influence, makes the victim implement the actions themselves (often seen in vishing fraud) (Krombholz et al, 2014; Zuoguang et al, 2021). Social engineering attacks exploits various human vulnerabilities such as emotions, cognition, personality traits and individual characteristics (Zuoguang et al, 2021). Emotions such as fear, impulsion, anger, and feelings such as sadness and guilt have a significant impact on cognition and decision-making on individuals, which can be exploited as vulnerabilities in social engineering attacks. For example, the victim may experience fear of not complying to what "authorities" say, and in the case of vishing frauds, fear is often used as an approach to gaining access to sensitive information. When provoking such emotions and feelings, the victim's cognitive ability can be held back and suppressed. Further, individual personality traits, to a large extent, affect the victims' susceptibility of being exploited by social engineering through misguidance, manipulation, or other influences. For example, vulnerabilities such as conformity entails a susceptibility to a social engineering attack, meaning that inexperience and low awareness makes it easier to be exploited by attackers. Some individual characteristics are more desired by the attacker, for example that some individuals are more probable to follow authority figures, meaning that there is less chance that they will contradict what the "authority" (attacker) asks them to do. Further, credulity is another vulnerability that increases the likelihood of being targeted by a social engineering attack (ibid).

In addition to human vulnerabilities, the attack methods explain the procedure of how the social engineering attack is carried out, explaining how the attacker creates different methods in order to succeed in exploiting the various human vulnerabilities and to attain the aim of the attack. It describes the implementation of the attack, the driving force behind the attack and to what extent it is intended to succeed. However, the attack methods change over time, not least in line with the advancement and expansion of technology. Through this, attackers and fraudsters will persist in creating more developed and advanced attack scenarios, resulting in further attack methods (Zuoguang et al, 2021).

The third factor, effect mechanism, explains how attack methods exploit human vulnerabilities and how exploitation of the vulnerabilities leads to the attack occurring. Effect mechanism includes several different aspects such as persuasion, cognition, trust, and emotions, each of them being important aspects for a

successful attack. By manipulating the victims' emotions, the attacker will be able to affect the victims' decisions, this in turn can lead to a change in the victim's way of thinking and acting since changed and affected emotions can influence a change of thoughts and choices (ibid). Specific methods explaining this is cognitive emotion regulation which describes the conscious, cognitive way of managing the consumption of emotional information and tasks. Previous research shows that regulation of emotions by cognitions helps people to keep control over their emotions during or after the experience of threatening or stressful events (Garnefski & Kraaij, 2007). One aspect mentioned is persuasion, common in vishing fraud is that the fraudsters often state calling from different authorities in order to exploit individuals' trust in authorities and through persuasion and manipulation achieves financial gain (Brå, 2020). Research has shown that obedience to authority can be so strong that our rational behavior and independent thinking risks being held back and subdued (Zuoguang et al, 2021). An additional aspect within effect mechanism is the impact of time pressure during a social engineering attack. Being exposed to time pressure can result in experiencing nervousness and stress which inhibits cognition and affects the victims logical thinking, thus increasing the risk for additional vulnerabilities, which generates greater chances for the attacker to succeed in convincing and manipulating the victim (ibid). As mentioned earlier, this approach is often used in vishing fraud (Säkerhetskollen, 2020). When referring to vishing attacks, or even social engineering attacks in general, the attacker must appear trustworthy towards the victim, since trust is a crucial factor that predicts the victims' propensity to be affected. In some situations, where specific factors have occurred that could deter a social engineering attack, the attack has still happened due to the high level of trust that has been created. Due to the importance of trust in order to accomplish an attack, attackers often attach significant importance to factors affecting this (Zuoguang et al, 2021). In conclusion, it can be stated that with the advancement and change of e.g., global technology, attackers will create new attack methods where further effect mechanisms are discovered and human vulnerabilities continue to be exploited (ibid).

2.3 The COVID pandemic as a tool for fraudsters

Like previous societal events or crises, the COVID pandemic has been exploited by fraudsters for the purpose of deceiving people (Police, 2020). The Swedish Police Authority and the Swedish public health authority have warned of various approaches and motives that have been COVID related. Linked to different stages during the pandemic, such as the emergence of the vaccine, several approaches have consisted of fraudsters who claim they are calling from the public health authority, 1177 or home care services, to get the victims to log in with their BankID and/or card reader or disclose other sensitive information (Säkerhetskollen, 2020b). The number of reports of fraud linked to the vaccine increased by 60% in February 2021 compared to January the same year (Säkerhetskollen, 2021). The approaches used by the fraudsters have been through both vishing and, in an extended scenario, also home visits (ibid). The police authority has warned of several motives given by fraudster in order to conduct home visits, such as vaccination offers (Säkerhetskollen, 2020b). To succeed in convincing the victim even more, there have been occasions where the fraudster says that a licensed doctor will accompany the visit (Säkerhetskollen, 2020b). Home visits, however, are not a new phenomenon and have been seen

prior to the pandemic with references to e.g., anti-theft marking (Säkerhetskollen, 2020). Whatever the stated reason, the intention is always the same, to obtain confidential, financial, and/or personal information.

In 2020, The National Operations Department (Noa) issued a report on the long-term consequences of the COVID pandemic on crime development, which presented that the number of reports where the COVID-19 was used as a motive were fewer than previously predicted (Polisen, 2020d). In addition, many of the modes observed were versions of pre-existing approaches seen in previous frauds or scenarios. However, fraud against vulnerable groups such as elderly is henceforth a topical threat, and that authority fraud (through vishing) may continue to increase since people spend more time in their homes (ibid).

3 METHOD

In the following section the research method of the study will be presented. Further, selection, sample size and ethical considerations will be discussed in relation to the implementation of the study.

3.1 Research method

The study intends to analyze and examine how vishing fraud has been affected by the COVID-19 pandemic in Sweden. To be able to answer the study's purpose and stated questions a qualitative research approach was used. Qualitative research is suitable for the current study since it is often used for exploratory purposes, such as understanding underlying reasons and interpreting contexts or conceptions. It allows for gaining a more in-depth understanding or insight into specific areas of research (Miles & Gilbert, 2005). The data collection method used for the study was one-on-one, semi-structured interviews. Semi-structured interviews allow the interviewer to combine specific questions and themes with the interviewees' free narrative and reflection. When conducting such interviews, the interviewer uses predetermined questions, however, the semi-structured approach also allows the interviewer to take different directions and ask follow-up questions about areas of interest raised by the interviewee. Further, semi-structured interviews tend to include a combination of open and closed questions, often followed by questions that ask why or how (Williams, 2015).

3.2 Selection

The sample method for the study is purposive sampling which means that the selection is based on the researcher's own assessment for choosing the specific sample, meaning that the participants are selected with anticipation that they will provide the study with important information (Etikan et al., 2016). The selected interviewees were employees within a Swedish bank and within The Swedish Police Authority. Within the police authority, the interviewees worked at Nationellt bedrägericentrum, NBC (National Fraud Center), who work primarily with crime prevention measures, analysis, and method development. The interviewees within the bank worked at the bank's fraud department. The sample

consisted of six (6) individuals; four bank employees and two employees from NBC. All interviewees had work experience related to the subject linked to their present and/or previous workplace. The average working experience with fraud was 3.9 years. However, several of the interviewees have long-term experience (10+ years) within this field of work, such as anti-money laundering (AML), preliminary investigation leader, operational analyst, and other bank related work. Financial institutions such as banks as well as the police authority are considered the primary actors working with fraud and were therefore considered to be relevant to interview in order to achieve the purpose of the study.

3.2.1 Sample size

It was primarily the purpose of the study and the time limit that determined the number of interviewees that was considered reasonable. When implementing qualitative methods, transcription and analysis of the collected material requires time and accuracy (Bryman, 2008). Six interviewees were therefore considered a reasonable number to answer the purpose of the study and to achieve data saturation. If the selection is too small, there is a risk that the material obtained will not be representative and if the selection is too large, there is a risk that the analysis would have decreased in quality since it can be difficult to navigate the extensive material. According to Bryman (2008), there is also a probability that adding more interviewees and interviews would not necessarily generate more data, but rather repetitions of what has been mentioned in previous interviews. It is considered that the interviewees had similar qualifications and experiences, hence the data saturation is achieved more effective (ibid).

3.3 Procedure

The participants within the police authority were contacted through email and the interviews were performed through Zoom and over the phone. With the bank employees, in-person interviews were conducted at their workplace, while with one interviewee it was performed through Zoom. All interviews took between 25-35 minutes to complete; the average length of the interviews was approximately 25 minutes. The material was recorded with a phone after consent from the interviewee was given. The interviews were then transcribed verbatim. The interviews were first conducted in Swedish and then excerpts used in the quotations were translated to English. The content of the interview guide was designed in such a way so that it could be applied to both the police authority and financial institutions and included questions which referred to reasons why fraud through social manipulation increased in 2020, how the COVID pandemic has been exploited by fraudsters, and the pandemic's impact on future working methods (see appendix). The interview guide was primarily used to ensure that all themes were addressed during the interview, beyond that, the interviewees were asked to speak freely.

3.4 Method of analysis

Thematic analysis was used as the method for the collected material, which is a common approach when analyzing material in qualitative interviews. Thematic

analysis focuses on analyzing and identifying common themes within the collected material (Braun & Clarke, 2006). The study applies a semantic approach, where specific themes identify the meaning of the explicit data collected from the respondents (ibid). Further, the study applies an inductive approach, which means that the codes were derived from the interviewees' answers in order to create themes for a thematic framework in the analysis. In accordance with Braun & Clarke (2006) the process of a thematic analysis consists of six different steps. After the interviews had been conducted, the first step of the analysis is transcribing the material. Through transcription, it enables the researcher to thoroughly study the material, this is done based on the study's primary purpose and questions. Further, initial codes are identified and created, this is an important step in the analysis where the researcher adds the material into groups. These may consist of both longer paragraphs and shorter sentences. In the third step of the analysis, the codes are divided into identified themes, which include patterns of meaning in the material. These can involve both larger and broader themes but also sub-themes. The next step in the analysis consists of refining the selected themes, this means that some themes may be removed if not enough material supports them, some themes can be merged if they are considered coherent. The next step includes defining the selected themes, each theme is described in detail and in what way they contribute to the study's purpose and issues. Broad themes may touch on similar topics, in such cases it is beneficial to use sub-themes that help to structure the analysis. In the final phase all themes and sub-themes are elaborated, which enables a final research assignment or written account (ibid).

3.5 Ethical consideration

When conducting research, it is essential to reflect on ethical rules and approaches to ensure anonymity and protective coverage for the participants (Vetenskapsrådet, 2017). The researcher must therefore take ethical requirements such as confidentiality, consent, information and use into account (ibid). The information collected was treated confidentially and the interviewees were informed that all interviews were anonymous and that no names will be used in the completed results of the study. All participants were given an informational letter on the study in advance. For those interviews that were not conducted through Zoom or over the phone, the informants signed an informed consent that was submitted along with the information letter, this material was stored securely. All informants were asked about an oral consent to participate in the study and that I would be allowed to record the interview. All informants were also informed that it was voluntary to participate in the study. For two participants the interviews were conducted over the phone and through Zoom. Verbal consent was sought for these participants so that no written material coupling their participation in the study had to be sent over the internet, which potentially is insecure. All interviewees were informed that the study was conducted for educational purposes and that finished work will be published on Malmö University's portal DiVA, which means that it will be a public document. The informants were also informed that the recorded material is for scientific use only and that the recording will be deleted after the material has been analyzed. In all interviews, flight mode was activated on the phone used when recording, this to achieve the confidentiality requirement and to minimize the risk of the material being spread. Further, for the above study, the material collected is not considered

sensitive, since it does not include personal information and/or other ethically sensitive content and for this reason did not need to undergo an ethical review, however strict ethical guidelines were adhered to.

4 RESULTS

The following section will address the results of the study based on the material collected from the interviews and analyzed from the transcribed material. The results will be categorized and presented according to the themes identified from the transcribed material (see table 1 below). The interviewees will be referred to as NBC employee 1-2 and bank employee 1-4.

Table 1. Selected identified themes.

Themes	Changed lifestyles	Social manipulation/ (Social engineering)	Future perspective
Sub themes	Increased time spent home Home visits	Technological development Background information	

4.1 Changed lifestyles

2020, which was largely affected by the COVID pandemic, has had a significant impact on society and in the everyday lives of individuals, both socially and economically. As a result of the pandemic, several aspects such as social distancing, isolation and changed means of communication has meant a change in lifestyle - this change is believed to be a reason to why vishing fraud has increased. Furthermore, as a possible consequence of spending more time at home, many interviewees brought up home visits as an extended scenario of vishing fraud.

4.1.1 Increased time spent at home

A recurring theme, brought up by several interviewees, was that time spent in the home during the pandemic has increased significantly in comparison to previous years. Spending more time at home makes people more vulnerable in several ways.

> It could be due to the pandemic, people are at home more making it much easier to be deceived by something like this, also that you are at home with all your personal belongings, sitting at your computer, etc. Bank employee 4

One of the interviewees addressed that since many bank-related matters have needed to be conducted from home, rather than visiting e.g., bank branch, many

have had to rely on communication through other channels such as through digital means, which has been exploited by fraudsters who use this approach.

> You have become more forced to perform things/transactions yourself [...] by that I mean that you cannot meet physically via bank branches in the same way, etc., therefore you must rely on it occurring through other communication channels, which means that the fraudster gets a larger arena to act in. Bank employee 2

Due to changes in lifestyle and existing restrictions and recommendations that have resulted in a reduced physical interaction, it is reasonable to assume that individuals' health and well-being is affected. Several interviewees discussed that during the pandemic many feel lonely and excluded, which can be linked to the fact that the amount of time spent at home is significantly greater and that socializing has decreased in relation to previous years.

> [...] People are even more lonely due to the pandemic than they have been before, especially old people who are already vulnerable [...] Bank employee 4

> [...] I can imagine that more people are exposed to vishing fraud because they are at home to a greater extent, don't meet anyone else and may not have anyone around who can notice if something is wrong. It is also easier to deceive someone who is in a fragile situation and who has not socially met anyone for a long time [...] Bank employee 1

4.1.2 Home visits

A recurring and related theme discussed by the interviewees was the extended scenario of vishing fraud, referring to physical home visits. In addition to the above listed impacts of changed lifestyle, a specific feature which was highlighted was that fraudsters referred to corona related matters with the intention of conducting home visits. As mentioned previously, the Swedish Police Authority has reported on "corona fraudsters" who have exploited phases and occurrences of adverse events during the pandemic. Although home visits have occurred prior to the pandemic, the approach however has become more varied. This means that the pandemic has increased the various arenas for which fraudsters can exploit e.g., which authority they are coming from, etc.

> There is a greater accuracy that an individual you want to mislead is at home in the home environment, both vishing where you have access to your card reader or BankID and with reference to physical vishing, since those you want to deceive are to a greater extent at home, the first communication takes place through a phone call, in close proximity to this, another person is nearby of the victim's home, through misleading they give greater effect for each call - it can be seen in statistics in attempts and completed crimes, that there are more completed crimes especially when it comes to physical vishing - that is the situational description. NBC employee 1

It can be assumed that physical vishing has been more successful and is more possible due to people being at home (both related and unrelated to the pandemic).

> I think it has been seen in general with the physical vishing, with home visits as a result of everyone being at home. Vishing is based on a phone call and often

> the age of the victim, often older, fragile, and impressionable, this is when we mean vishing with the reason of wanting to conduct a home visit. NBC employee 1

> [...] More people are at home. Home visits are very good for fraudsters who have targeted the older generation, they have evidence and believe that it is reasonable for someone to come to their home. It's ingenious from the fraudster - some of the fraudsters have masks, making it hard to identify them [...] Bank employee 2

However, in terms of vishing fraud or the fact that the pandemic might have made elderly even more affected, it must be emphasized that elderly have always been a vulnerable and exposed group in this regard.

> [...] It is difficult to say whether it is due to the pandemic or that there are more fraudsters trying to commit crimes meaning that there are more crimes that are completed [...]. NBC employee 2

4.2 Social manipulation (Social engineering)

As stated above, an increase in fraud through social manipulation was noted both prior to and during 2020. The participants were asked what they considered to be the reasons behind this, more generally. Several interviewees highlighted the possibilities and the efficiency that social manipulation entails. As previously described, a key aspect of social manipulation is the exploitation of human vulnerabilities and the use of effect mechanisms such as persuasion and trust, in order to affect the victims' decisions (Zuoguang et al, 2021). The use of social manipulation has occurred regardless of the pandemic. However, the pandemic has impacted the lives of individuals; where more time has been spent at home and an increased demand for technical knowledge and different communication modes. This has expanded the arena for which the fraudsters operate within and hence increased their chances of succeeding in convincing and manipulating its victims. Nevertheless, the increase of social manipulations may well have happened even if the pandemic had not occurred, which, however, remains speculative.

> [...] The fraudsters know how to express themselves, what to emphasize in order to make the victim feel calm but still get the victim to perform as they want [...] Bank employee 3

4.2.1 Technology development

The technical possibilities and/or technological development such as an increased use of BankID and extended technical solutions for purchases and payments were addressed. The availability of technical tools such as number spoofing and how this is exploited by fraudsters in the context of social manipulation was brought up by the interviewees. Exploitation of trust and confidence in authorities was also a recurring theme.

> [...] Quite many years ago, the technical solutions were dominated by trojans, hacking, etc. Until the fraudsters realized that they can just call people and "ask" for their money and then they will get them [...] Bank employee 4

> [...] Primarily due to the general technical development and communication methods - technical solutions with how we communicate with each other where many age categories are represented, it is also the technical solutions with purchases and payments that opens a market for those who have crime in mind. The social in all contexts has been moved to move to technical means of communication and solutions [...]. NBC employee 1

> The variation has also become greater on who the fraudster represents themselves as, the police mode has for example existed for a long time, the spectrum from various "authorities" that contact the victims has however increased. NBC employee 1

Several interviewees highlighted that one of the reasons why fraudsters use social manipulation to a large extent, is because of their ability to take advantage of the technological benefits. One of the reasons why the fraudster can exploit these technical possibilities is because they adopt the same type of methods that banks and other authorities use in legitimate ways, for example the use of identification systems (e.g., BankID).

> They have found a way where technology is used so effectively through BankID, swish, spoofing etc. It is so easy to pretend to be the bank, but also that many banks use that verification method. Bank employee 1

> When technical security improves, it seems that fraudsters improve their social (engineering) skills in a different way, and persuade the victim to bypass the technical solutions, which is difficult to do in any other way if you do not have very broad technical competence itself. NBC employee 2

Since many services to a greater extent are digital today, this entails certain difficulties for elderly since many lack the knowledge and practical experience of digital means, such as BankID, swish etcetera. This means that they often are excluded from digital contexts. This is consequently exploited by fraudsters.

> [...] I think that it is partly because the technology is developing so fast, many older people who are exposed to vishing do not keep up and do not understand how for example swish works, swish is often used in vishing fraud [...] Bank employee 1

> [...] Elderly has a harder time keeping up with technology in the same way as younger people. Many fraudsters use technical tools such as spoofing - meaning that they are often technically proficient [...] Bank employee 3

4.2.2 Background information

The availability of personal data and background information of the victim was discussed by several participants. However, these issues have occurred separately but in concurrence with the pandemic, and hence it is of relevance to this study and its context of the COVID pandemic. Several described, based on experience, that the fraudsters over recent years have evolved by becoming more personal and often having a lot of information about the victim prior to the fraud, in many cases causing the victim to act in accordance with the fraudsters' instructions. Further, they described the importance of fraudsters obtaining extensive background information of its targeted victims and the chances of succeeding in a vishing fraud, which coincides with NBC's information (Sveriges Radio, 2021, 12:10).

> [...] When talking to customers who have been exposed to vishing fraud, it turns out that many fraudsters tell them about their marital status, social security number, addresses etc. They also tend to know different bank details, they can guess which bank they belong to by checking which bank branches are nearby etc. [...] Bank employee 1

> [...] Many do not know how easy it is to get hold of personal information, it is probably not that they are easily accessible, but rather that people do not know how easily accessible it is - so if someone (fraudster) calls and knows something personal about them, then they assume that it is correct, since they would not know it otherwise. If people knew how easily accessible it was… [...] Bank employee 4

One of the interviewees explains, as also mentioned earlier, that background information is often used in vishing fraud as an important factor in appearing convincing, and thus to some extent increases the chances that the fraud succeeds. However, the same interviewee emphasizes that depending on the victim's receptivity, the fraudsters tend to adapt to this and change their approach. This emphasizes how fraudsters are prone to change.

> [...] I think the fraudsters are so flexible that when they have a victim, they are quite open in their conversation about what could happen - depending on how receptive the victim is [...]. NBC employee 2

4.3 Future perspective

The interviewees were asked if their gained experience of the pandemic could affect future work, referring to; cooperation between authorities, changes in crime, working methods, exploitation of societal crises etc. Interviewees from both institutions emphasized the importance of a continued and extended cooperation between involved parties such as financial institutions and The Swedish Police Authority. Further, several participants mentioned that the COVID pandemic to some extent has brought new knowledge about the topic discussed and that the knowledge could/should be used for future similar events. Since the COVID pandemic eventually will subside, this means that the reference to COVID-19 will no longer have an effect to the same extent. Fraudsters will therefore change to new ways of exploiting, whereupon it has highlighted that future focus should be to change and improve working methods according to how the fraud occurs and how the fraudsters operate.

> [...] A broader mapping means that we can change our way of working according to how the frauds occurs [...] we must be proactive before the next fraud occurs [...] with vishing fraud, the fraudsters tend to change very quickly [...] Bank employee 3

> [...] Maybe not directly the covid pandemic, but rather the work with collaboration and the working methods that we will work with in the long term in the future, and when it comes to the parts with the financial institutions where we have not come very far together to share that we have a picture of the situation, but we must see and share the same pictures of the situations [...] There is a need to work more in those forms, it is about the total impact of resource allocation and crime profits and where they go [...] NBC employee 1

Further, the importance of cooperation is described as follows:

> [...] It is fundamental that we have good contact between banks since when it comes to vishing the money goes very quickly [...] then the police's efforts means very much so the cooperation between the bank and the police in those cases are very important and I think that there is much more that can be done there [...] Bank employee 1

5 DISCUSSION

In the National Operations Departments (Noa) report on the long-term consequences of the COVID pandemic for crime development, it has been described that social distancing, limited interaction, and the fact that more and more is done at a distance has led to an increased use of digital solutions and an increased need for communication over the internet. This implies an increased number of potential victims and crime opportunities. Noa states that this can primarily be linked to cybercrime (Polisen, 2020d). Based on this study however, it can be argued that it can also be applied to vishing fraud. In addition to the above and in accordance with Brås statistics, an increase in fraud through social manipulation has been noted during 2020 in comparison to previous years. For some modes an increase could be noted during all the pandemic months compared to the equivalent months during 2019. However, an increase in fraud through social manipulation such as vishing could be noted even prior to the pandemic (significant increase in vishing fraud was seen already in 2018). Brå therefore concludes that the increase cannot be stated to be due to the pandemic, however, believes that such conclusions cannot be excluded either (Brå, 2021). Although the increase cannot exclusively be explained by the pandemic, it is clear that the pandemic has been exploited by fraudsters in different ways. Several approaches and procedures have been seen as being directly linked to the pandemic, where the fraudsters use the coronavirus and/ or COVID-19 to deceive the victims to obtain financial gain (SOU 2020:09). However, many of the procedures that fraudsters have used during the pandemic, are methods that have been used in previous years. Meaning that the fraudsters have adapted existing modes with COVID-19 features (Polisen, 2020d). According to a report by the Statens offentliga utredningar, SOU (State Public Investigations) states that there are difficulties in being able to determine whether differences in crime statistics between years and/or changes in crime are due to the COVID pandemic as there are several different aspects that may have had an impact and therefore needs to be considered. The report therefore emphasizes the importance of not only considering crime statistics or its direction in order to be able to determine whether the possible change is due to the pandemic or not. It is further explained that it is common in crime statistics that the number of reports fluctuates and that differences in statistics between previous years have been both larger and smaller than the differences during the pandemic year and the year before. Meaning that it is difficult to determine whether changes could be affected by the pandemic or if such changes had occurred independently of the pandemic and/or with other influential societal factors. Hence it is too early to draw more comprehensive conclusions about the consequences of the pandemic and what possible consequences it could have on crime. Due to the several different circumstances mentioned above, and that the pandemic is still ongoing it is reasonable to assume that its impact has not yet subsided. This means that most of the observations to

this date are preliminary, due to substantial data not yet collected and analyzed. Thus, authorities emphasize that a longer time perspective is needed to verify the preliminary conclusions and/or enable for new ones (SOU 2020:09).

Furthermore, the COVID pandemic has caused a change in life patterns for individuals and when such factors are affected and changed, it is reasonable to assume that crime adapts and exploits these changes (ibid). Due to limited interaction, increased time spent at home and the extended use of communication via digital means, suggests that fraudsters have been given a larger arena through which they can commit vishing fraud. In this context, the routine activity theory can be applied, meaning that in those contexts where the interaction increases and where the absence of control exists, the incidence of crime increases (ibid). This could explain the occurrence of home visits during the pandemic, and to some degree the common denominator regarding the lacking absence of control - meaning that the pandemic has created special conditions which are not common and thereof can be utilized. As mentioned above, technological development, the increased use of technical tools and the fact that elderly are alone to a greater extent during the pandemic were discussed as reasons why vishing fraud has increased during 2020. It was discussed how isolation of elderly during the pandemic exposed them to a greater extent. However, elderly have always been a vulnerable group targeted by fraudsters for such reasons. Furthermore, the majority of elderly have never been 'part of' the digital society, and thus have less understanding of digital means such as BankID. Furthermore, its exclusion may be due to lack of ability and/or motivation (Folkhälsomyndigheten, 2018). These factors expose elderly even more, as they are forced to adapt or risk being an easy target for fraudsters. This, what could be deemed as a problematic development in this regard, has existed prior to the pandemic. However, the exposure of elderly during societal changes (either technological or as of now the pandemic) has become more evident.

A recurring theme that was discussed by the interviewees in relation to the emergence of vishing fraud both before and during the pandemic was social manipulation. In previous research, it is emphasized that certain human vulnerabilities increase the risk of being exposed to a social engineering attack. Inexperience and/or low awareness are examples of such vulnerabilities (Zuoguang et al, 2021). Based on the interviewees' answers, this could be applied to elderly based on their general knowledge and experience of digital means and the demands that have been placed on this during the pandemic. Further, a key aspect of effect mechanism, as mentioned, is trust. Based on previous research and the interviewees' answers, it appears that the variation in who the fraudsters claim to represent have become increasingly varied. Thus, it can be assumed that the pandemic has increased the possibilities for who the fraudsters can claim to represent, and thereby exploit people's trust in authorities. Furthermore, it can therefore be assumed that changes caused by the COVID pandemic creates opportunities for fraudsters which they exploit. However, fraudsters tend to be flexible in nature and hence it can be assumed that other coincidences would have been exploited if the pandemic had not occurred.

In conclusion, it is reasonable to assume that changes and differences in crime levels most often are caused by several different factors combined. Hence it can be concluded that a noted increase in fraud through social manipulation such as vishing fraud does not exist solely because of the pandemic or other individual

causes. However, issues like pandemics and other crises are clearly prime grounds for various new and innovative forms of fraud, and authorities perhaps need to see what is happening during this current one and help it guide responses in the future for these issues.

5.1 Suggestions for future research

It would be of relevance to further examine the effect of the COVID pandemic on vishing fraud or on crime in general after its end, when the consequences of it may have become more noticeable. A possible effect of the pandemic is believed to be a recession, which according to existing research might affect crime more than the pandemic itself (SOU 2020:09).

6 LIMITATIONS

In terms of sample size, I acknowledge that the sample was small but thus believe their specialized expertise would provide in-depth knowledge, however, there is a risk of missing out individuals who could hold other experiences and knowledge. Furthermore, it may also have been possible to perform questionnaires, which might have contributed to more general knowledge, however, this method was not included, since it was in-depth knowledge that was sought in this study. As stated, vishing fraud occurs both globally and nationally. Although it is a global occurring issue, the following study was limited to a Swedish context, since the interviews were conducted with individuals who work within this context. Comparisons in the study were made mainly based on statistics from Brå, which meant that comparisons with international statistics were not made to a greater extent, since such comparisons had required a separate study. Another limitation in the study was that all interviews were conducted in Swedish, after which all excerpts were translated into English. This may entail certain limitations such as incorrect translations and thus incorrect results etcetera. However, I am fluent in both languages so this should not present a problem. Furthermore, it needs to be addressed that I had previous knowledge about some of the individuals who took part in the interview. This can be seen as an advantage if it made the interviewees feel more secure which thus benefits the interview. However, it may also have been a disadvantage if it affected the ability of those involved to stay objective during the study. Finally, it is important to highlight that although vishing fraud primarily affects elderly, other groups are also affected. However, due to the time and space limitations of this study, this was not addressed.

7 CONCLUSIONS

This study has provided an analysis of how vishing fraud have been affected by the COVID pandemic and what factors can explain the increase in fraud through social manipulation. Changed lifestyle has meant increased time spent at home, which was discussed as one of the reasons that makes the victim more receptive. Further, technical development and the possibilities that follows with it, and the

efficiency that social manipulation entails was discussed by the interviewees as a cause for its increased usage. The study also examined whether the pandemic has affected or influenced future working methods or created new insights for the parties concerned. It was emphasized that since the pandemic will subside, this means that the reference to COVID-19 will no longer have an effect and fraudsters will change to new ways of exploiting. Hence it was highlighted that future focus should be to change and improve working methods according to how the frauds occurs and how the fraudsters operate. Furthermore, although cooperation between authorities and financial institutions is valued, its relevance has been further highlighted during the pandemic, concerning both the investigative- and crime prevention work.

Due to a noted increase in fraud through social manipulation such as vishing fraud prior to the pandemic, it has not been possible to determine whether a further increase is due to the pandemic or not. Based on this study it is considered too early to conclude about the pandemic’s exact consequences and its impact on crime. The research further concluded that the COVID pandemic has been used by fraudsters to some extent where several motives have been directly linked to the pandemic and where the fraudsters have used COVID-19 to deceive the victims. Thus, from a criminological perspective, it opens up for supplementary and further research about the pandemic's direct and indirect effect on crime, people's well-being, health and everyday life.

REFERENCES

Braun, V., Clarke, V. (2006). *Using thematic analysis in psychology.* Qualitative Research in Psychology, 3 (2). pp. 77-101. ISSN 1478-0887

Bryman, A. (2008). *Samhällsvetenskapliga metoder.* Liber AB.

Brå. (2019). *Kriminalstatistik 2019 Anmälda brott - Preliminär statistik första halvåret 2019.* Brottsförebyggande rådet. https://www.bra.se/download/18.62c6cfa2166eca5d70e350cd/1614335518929/Sammanfattning_anmalda_prel_halvar_2019.pdf (Accessed 2021-02-03).

Brå. (2020). *Bedrägerier och ekobrott.* https://www.bra.se/statistik/statistik-utifran-brottstyper/bedragerier-och-ekobrott.html (Accessed 2021-01-30).

Brå. (2020a). *Kriminalstatistik 2020 Anmälda brott - Slutlig statistik.* https://www.bra.se/download/18.1f8c9903175f8b2aa707e2d/1617086483071/Sammanfattning_anmalda_2020.pdf Brottsförebyggande rådet. (Accessed 2021-05-11).

Brå. (2020b). *Ekonomisk brottslighet.* https://www.bra.se/forskning-och-analys/ekonomisk-brottslighet.html (Accessed 2021-02-03).

Brå. (2021). *Fortsatta indikationer på konsekvenser av pandemin i Brås preliminära statistik över anmälda brott i november 2020.* Brottsförebyggande rådet. urn:nbn:se:bra-949

Elliott, R., Timulak, L. (2005). Descriptive and interpretive approaches to qualitative research. In Miles, J., Gilbert, P. (ed.). *A handbook of research methods for clinical & health psychology.* Oxford university press, p147

Etikan, I., Musa, S., Alkassim, R. (2016). *Comparison of Convenience Sampling and Purposive Sampling. American Journal of Theoretical and Applied Statistics.* Vol. 5, No. 1, 2016, pp. 1-4.

FBI. (2020). *Money Mules.* https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules (Accessed 2021-02-26).

Folkhälsomyndigheten. (2018). *Digital teknik för social delaktighet bland äldre personer. Ett kunskapsstöd om möjliga insatser utifrån forskning, praktik, staktik, juridik och etik.* Artikelnummer: 18063. Folkhälsomyndigheten, Forte, Socialstyrelsen, Statens beredning för medicinsk och social utvärdering och Myndigheten för delaktighet. (Accessed 2021-05-13).

Garnefski, N., Kraaij, V. (2007). *The Cognitive Emotion Regulation Questionnaire - Psychometric features and prospective relationships with depression and anxiety in adults.* European Journal of Psychological Assessment 2007; Vol. 23(3):141–149. Hogrefe & Huber Publishers

Hadnagy, Christopher. (2018). *Social Engineering: The Science of Human Hacking.* John Wiley & Sons, Inc

Handels. (2018). *Ekobrottsligheten i handeln - En genomgång och analys av brott som drabbar välfärdssamhället.* Handels Rapportserie 2018:1. https://handels.se/globalassets/centralt/media/pressrum/rapporter/2018/rapport--ekobrottlighet-i-handeln-2018.pdf (Accessed 2021-02-01).

International compliance association. (2020). *What is Financial Crime? | ICA.* https://www.int-comp.org/careers/your-career-in-financial-crime-prevention/what-is-financial-crime/ (Accessed 2021-05-03).

Interpol. (2020). *Financial crime.* https://www.interpol.int/Crimes/Financial-crime (Accessed 2021-02-02).

Kantar Sifo. (2020). *Anseendeindex Myndigheter 2020.* Sifo. https://www.kantarsifo.se/rapporter-undersokningar/anseendeindex-myndigheter-2020 (Accessed 2021-02-25).

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). *Advanced social engineering attacks.* Journal of Information Security and Applications, 22, 113-122.

McKinsey & Company. (2019). *Financial crime and fraud in the age of cybersecurity.* https://www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity (Accessed 2021-02-01).

NE Nationalencyklopedin (2021). *Vishing.* https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/vishing (Accessed 2021-02-01).

Operation Casino. Episode 1-3. (2021). TV4 Play, 15 February. https://www.tv4play.se/program/operation-casino

Polisen. (2016). *Nationellt bedrägericenter: Intressant just nu om bedrägerier.* Polisen. https://insynsverige.se/documentHandler.ashx?did=1856040 (Accessed 2021-05-20).

Polisen. (2019). *Telefonbedrägerier - skydda dig.* https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/bedrageri/telefonbedragerier---skydda-dig/ (Accessed 2021-05-19).

Polisen. (2020). *Bedragare utnyttjar corona för att lura äldre.* https://polisen.se/aktuellt/nyheter/2020/mars/bedragare-utnyttjar-corona-for-att-lura-aldre/ (Accessed 2021-02-07).

Polisen. (2020a). *Skydda dig mot vishing.* (Accessed 2021-02-26).

Polisen. (2020b). *Tänk säkert och skydda dig mot Vishing.* https://polisen.se/aktuellt/nyheter/2020/oktober/tank-sakert-och-skydda-dig-mot-vishing/ (Accessed 2021-02-26).

Polisen. (2020c). *Sverige i internationell insats mot bedrägerier.* https://polisen.se/aktuellt/nyheter/2020/december/sverige-i-internationell-insats-mot-bedragerier/ (Accessed 2021-02-03).

Polisen. (2020d). *COVID-19. Pandemins långsiktiga konsekvenser för brottsutveckling och samhällsordning.* Nationella operativa avdelningen Underrättelseenheten A141.490/2020

Polisen. (2020e). *Corona-bedragare i Farsta i södra Stockholm.* https://polisen.se/aktuellt/nyheter/2020/mars/corona-bedragare-i-farsta-i-sodra-stockholm/ (Accessed 2021-02-07).

Polisen. (2020f). *Telefonbedrägerier mot äldre ökar igen.* https://polisen.se/aktuellt/nyheter/2020/december/telefonbedragerier-mot-aldre-okar-igen/ (Accessed 2021-05-19).

Regeringskansliet. (2014). *Offentlighetsprincipen.* https://www.regeringen.se/sa-styrs-sverige/grundlagar-och-demokratiskt-deltagande/offentlighetsprincipen/ (Accessed 2021-03-10).

SOU 2020:09. *Coronapandemin, brottsligheten och rättsväsendets myndigheter.*

Sveriges radio. (2019). *Operation Dimma ska stoppa bedrägerier mot äldre.* https://sverigesradio.se/artikel/7132067 (Accessed 2021-05-20).

Sveriges radio. (2021). *Nätverkens oväntade inkomstkällor.* https://sverigesradio.se/avsnitt/1656000 (Accessed 2021-04-13).

Svensk Handel. (2020). *Signatur vid kortköp nekas från och med 1 november.* https://www.svenskhandel.se/radgivning/betalfragor/inte-langre-giltigt-att-godkanna-kortkop-med-signatur/ (Accessed 2021-03-29).

SVT Nyheter. (2020). *Vishing finansierar grovt kriminella gäng i Östergötland.* https://www.svt.se/nyheter/lokalt/ost/vishing-finansierar-grovt-kriminalla-gang-i-ostergotland (Accessed 2021-02-01).

SVT Nyheter. (2021). *Polisen varnar för bedragare som riktar in sig på äldre.* https://www.svt.se/nyheter/lokalt/orebro/polisen-varnar-for-bedragare-som-riktar-in-sig-pa-aldre (Accessed 2021-03-18).

Säkerhetskollen. (2020). *Vishing.* https://sakerhetskollen.se/sakerhetsguider/vishing (Accessed 2021-02-07).

Säkerhetskollen. (2020a). *Brottsstatistik över bedrägerier 2020.* https://sakerhetskollen.se/artiklar/brottsstatistik-over-bedragerier-2020 (Accessed 2021-04-06).

Säkerhetskollen. (2020b). *Varning för vaccinationsbedrägerier*. https://sakerhetskollen.se/artiklar/varning-for-vaccinationsbedragerier (Accessed 2021-02-26).

Säkerhetskollen. (2020c). *Multikriminella nätverk fokuserar på bedrägerier.* https://sakerhetskollen.se/artiklar/multikriminella-natverk-fokuserar-pa-bedragerier (Accessed 2021-03-20).

Säkerhetskollen. (2021). *Många bedrägeriförsök i samband med vaccinering.* https://sakerhetskollen.se/artiklar/manga-bedrageriforsok-i-samband-med-vaccinering. (Accessed 2021-05-07).

Vetenskapsrådet. (2017). *God forskningssed.* ISBN 978-91-7307-189-5

William, A. (2015). *Conducting Semi-Structured Interviews.* Handbook of practical program evaluation. Fourth edition. Jossey-Bass

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). *Phishing, Smishing & Vishing: an assessment of threats against mobile devices.* Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297-307.

Zuoguang, W., Hongsong, Z., Limin, S. (2021). *Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods.* IEEEAccess. VOLUME 9, 2021

APPENDIX

Describe your work and how it is related to fraud? How long have you worked with fraud? Describe your experiences of working with fraud.

Vishing fraud have shown an upward trend in 2020, what do you think are the reasons for this?

What do you think is the reason why the number of vishing fraud in 2020 has had an upward trend while remaining frauds have shown a downward trend? What different factors can explain this?

In what ways have vishing fraud been affected by the COVID pandemic? Why?

Fraud through social manipulation is increasing, what do you think are the reasons for this? Why?

If/how has the police authority/bank had to work differently with vishing fraud during the COVID pandemic in relation to prior years?

Do you think the impact of the COVID pandemic will result in the police authority/banks future work on vishing frauds changing? How? Why?