CYBERCRIME USING ELECTRONICAL IDENTIFICATION

WHAT ARE THE DANGER FOR CRIMINALITY?

ELEONOR BRANDT HJERTSTEDT

Degree Project in Criminology
Advanced Level 30 Credits
Two-year Program Master of Criminology
May 2019

Malmö University
Health and Society
205 06 Malmö

BROTTSLIGHET PÅ NÄTET VID ANVÄNDNING AV ELEKTRONISK IDENTIFIKATION

VAD ÄR RISKEN FÖR KRIMINALITET?

ELEONOR BRANDT HJERTSTEDT

Brandt Hjertstedt, E. Brottslighet på nätet vid användning av elektronisk identifikation. Vad är riskerna för kriminalitet? *Examensarbete i kriminologi 30 högskolepoäng*. Malmö universitet: Fakulteten för hälsa och samhälle, institutionen för Kriminologi, 2019.

Detta examensarbete undersöker riskerna med elektronisk identifiering, mer specifikt säkerhetsrisker kring enheten BankID i Sverige. Idag används BankID i stor utsträckning, men elektronisk identifiering kommer också med vissa risker när det gäller identitetsrelaterade brott. I Sverige var brottstypen som ökade mest det senaste året mätt i anmälda brott, bedrägerier som huvudsakligen begåtts genom informationsteknik (Brottsförebyggande rådet 2019). Arbetet syftar därför till att undersöka vilka säkerhetsrisker som finns med den elektroniska identifieringen BankID, och hur Polismyndigheten och Ekobrottsmyndigheten bekämpar brott på detta område. Resultatet visar att den största säkerhetsrisken med BankID är användare/kunder som kan luras. Gärningsmän använder olika metoder för att få tillgång till andra personer BankID. Vad gäller hur Polismyndigheten och Ekobrottsmyndigheten bekämpar brott riktade mot elektronisk identifiering är resultatet delvis bristfälligt på grund av att Ekobrottsmyndigheten inte är representerade. Utifrån polisens perspektiv så undersöker de bedrägeri avseende BankID så som de gör med alla andra brott, men brottet har generellt en lägre prioritet inom myndigheten. Polisen samarbetar med olika aktörer samt bidrar båda till att utveckla produktens säkerhet och informera kunderna om säkerhet och risker avseende BankID.

Nyckelord: BankID, Bedrägeri, Elektronisk identifikation, Internetrelaterad brottslighet, Olovlig identitetsanvändning.

CYBERCRIME USING ELECTRONICAL IDENTIFICATION

WHAT ARE THE DANGER FOR CRIMINALITY?

ELEONOR BRANDT HJERTSTEDT

Brandt Hjertstedt, E. Cybercrime Using Electronical Identification. What are the Danger for Criminality? *Degree project in Criminology 30 credits*. Malmö University: Faculty of Health and Society, Department of Criminology, 2019.

This thesis investigates the threats against electronical identification, more specifically the danger that comes with the device BankID in Sweden. Today BankID is widely used but electronical identification also comes with certain security risks regarding identity related crimes. In Sweden, the crime type which increased the most last year 2018 measured in reported crimes was fraud mainly committed through information technology (Brottsförebyggande rådet 2019). This thesis therefore aim to investigate what the safety risks are using electronical identification, such as BankID and how the police force and Swedish Economic Crime Authority combat cybercrimes in this area. The result show that the main security risk with BankID is the customers that can be deceived. Perpetrators use different methods to get access to another individuals BankID. Regarding how the police force and Swedish Economic Crime Authority combat crimes against electronical identification, the result is partly defective due to that the Swedish Economic Crime Authority not being represented in this thesis. However, from the police perspective, they investigate fraud regarding BankID as all other crimes but it has in general a lower priority within the authority. The police cooperate with different actors and help both with development of the product security and inform customers about safety and risks regarding BankID.

Keywords: BankID, Cybercrime, Electronical Identification, Fraud, Identity Fraud, Identity Related Crimes, Identity Theft.

TABLE OF CONTENT

INTRODUCTION

This thesis investigates the threats against electronical identification, more specifically the danger that comes with the device BankID in Sweden. Today BankID is used when confirming one's identity, for example when signing into a portal to see one's medical journal, paying taxes or paying electronical bills via private websites (BankID 2019). There are many benefits using electronical identification and it is widely used, however identification electronical also comes with certain security risks regarding identity related crimes. The Police Authority reported 2017 that many perpetrators try to steal others BankID which can besides give these perpetrators financial benefits, also the possibility to get access to important and sensitive information such as to make changes in public records, payments and pension savings (Polismyndigheten 2017). Identity related crimes occur across national borders and is a challenging problem. When it comes to the legal system and law enforcement, identity related crimes challenge authorities to be updated and multi-disciplinary in a legal perspective to promote alliance between nations (Cassim 2015). On the other hand, research implies that method aiming to combat identity related crimes in an electronical aspect is contested and do not always target the problem at its core (Koops 2009).

Identity related crimes is a part of a bigger concept called cybercrimes. The term 'cybercrime' encompasses "all forms of criminal activity perpetrated using information technology and the Internet" (Mehan 2014, p.67). Recently, there seem to be a shifting trend from traditional crime types to cybercrimes (Dobrinoiu 2014). Today, cybercrime is one of the largest pressing concerns facing the digital world (Moskowitz 2017). Cybercrimes defines the use of computer to commit illegal acts. There are different types of cybercrimes. Cybercrimes regarding BankID are both for example crimes against property as fraud, but it can also be identity theft, meaning that someone is using another person's identity (Brenner 2012). Finally, although there are certain risks with using electronic identification, the device is still largely used around the country. The News Bank stressed in an article published 2014 that BankID was stated as the most common method in Sweden for citizens when filing for tax returns (Adams 2014). This trend has sustained, and in 2018 the number of applications made with BankID (both logins and signatures) amounted to 3,3 billion, of which Mobile BankID stood for 96 per cent of the applications. Out of Sweden's population, 97,5 per cent among the individuals between 21 and 50 years had one or more BankID measured in November 2018 (BankID 2018).

Aim

The aim of this thesis is to investigate cybercrimes against electronical identification by using BankID as the main case study. The risks for cybercrimes which the technology is giving rise to, will be identified, mapped and analysed. Also, the thesis will investigate how the Police Authority and Swedish Economic Crime Authority (Ekobrottsmyndigheten) are combatting cyber financial crimes.

Research Questions

- What are the safety risks using electronical identification, as BankID?
- How does the Swedish Police force and Swedish Economic Crime Authority combat cybercrimes in this area?

BACKGROUND

Recently, there seem to be a shift in traditional crime types to another form called cybercrimes. These conclusions are mainly drawn from crime statistics showing that the crime rate has not fallen but instead changed to newer crime involving information technology (Dobrinoiu 2014). As for Sweden, the crime type increasing the most last year 2018 measured in reported crimes was fraud mainly committed through information technology (Brottsförebyggande rådet 2019). These forms of crimes take place in a digital world and, compared to more traditional crimes, not attached to physical convergence in time and space of victim and offender (Kranenbarg et al. 2017). One part of cybercrime is identity related crimes that are a wide concept defining identity deletion to illegal identity creation and identity theft (Koops 2009). Identity related crimes has arisen from the use of electronic services partly provided by the banking sector. E-banking system allows people and business to obtain personal information and do financial transactions using electronically identification. However, in line with this transformation comes the importance of security since perpetrators take advantage of the growing dependence on technology (Waller, Bailey & Johnson 2015).

BankID

BankID or bank identity is an electronical identification devise functioning as data file or as a mobile application. Some of the largest banks in Sweden introduced BankID in 2003 and it has now growth to eleven banks issue BankID to their customers. In Sweden banks are the providers and validators, and therefore each individual need to apply to the bank for an approval to use BankID (BankID 2019). There are few alternatives to BankID in Sweden and today many people in Sweden uses BankID for financial purpose or to issuing identity documents with public authorities. BankID can therefore be viewed as a multiple electronical identification system used for various purposes (Husz 2018). When it comes to BankID that is an electronical identification, there also exist a risk for identity theft that are action committed using electronics to take over and illegally acquire further use of a person's identity to commit other offences (Dobrinoiu 2014).

Legal Perspective

In Swedish legal system, fraud is stated in the code validation (BrB 9 kap 1§) which means that someone has tricked another person to do or not to do something that will benefit the perpetrator economically and the victim will instead suffer economically. In 2016, a new legislation entered into force, namely unlawful identity use (*olovlig identitetsanvändning*) (BrB 4 kap 6b§; Law 2016:485). This law applies to individuals who unlawful uses another person's identity by for example using BankID in purpose to take loans in that person's name. Another relevant legislation to BankID also introduced in 2016 was Law (2016: 561) with supplementary provisions to the EU regulation on electronic identification (*Lag 2016:561 med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering*) which describes the guideline for electronical identification (Sveriges Riksdag 2016). Relevant to this legislation is an indicative judgment that can be found established by the Swedish Supreme Court concerning electronic identification, verdict NJA 2017 s.1105. Electronic identification is stated as an identity only for the consumer's purpose. The burden of proof regarding the security of the technical product that provides electronical identification, lies with the party providing the product. Conversely, there may be uncertainties regarding who has signed the electronic identification. The owner of

the electronical identification must somehow prove that he or she has protected the bank code and has a safe equipment but also that another person has used the electronical identification without consent or knowledge. The agreement between provider of BankID and the user must be safe, so that both parties can trust the electronical signing.

THEORY

Crimes regarding identity theft is often referred as a white-collar crime. The difference between traditional crime and white-collar crime is not quite clear today, and some researchers question if white-collar crime could be defined as a unique offence with its own theoretical ground (Piquero 2018). The terminology of white-collar crime has been defined by Edwin H. Sutherland in the 1940 as an attempt to explain that anyone can commit criminal offences regardless of social class. Sutherland saw a need in criminology research regarding theory applying to all social classes and not only lower- or middle class criminality that has been the focus for many criminologists (Sutherland 1940).

As Sutherland explains "White-collar criminality is real criminality, being in all cases in violation of the criminal law" (Sutherland 1940, p.11). This theoretical explanation may be quite fair. It seems that most individuals that commit identity theft and are convicted, often comes from working-class and middle-class backgrounds. The characteristics of identity theft offenders are divided. There are those who is similar to street crime offenders and those that seem to be more privileged (Copes & Vieraities 2007). Identity theft offenders seem to come from a wide range of family backgrounds, lifestyle and criminal history. A common motive for committing identity theft is often a need for quick money. The information needed for stealing identity such as names or addresses can be bought from someone else or the offender is using more sophisticate methods to hack computer systems or trick people to give their personal information regarding their ID. Often, these perpetrators are targeting information or victims that they can access or approach more easily, or they might seek vulnerabilities in the networks that provides sensitive information (ibid).

Another criminological theory that has been applied on identity theft, is the routine activity theory. This theory was developed by Cohen and Felson (1979) in order to explain how opportunity to commit crimes is dependent upon human routine activities. This theory states that it is people's routines, movement patterns and land use that are the basis for why crime differs between different parts of a city (ibid). The theory has moreover been developed in research by Felson and Boba (2010) who explained hot spots such as shopping centres and bars that increase the possibility of crime due to the fact that there are attractive crime objects. People also tend to commit crimes in areas where there is a small risk of being detected (ibid). However, when it comes to identity theft online, the perpetrator and the victim is rarely direct-connected. Instead the crime occurs online when the perpetrator get a hold of the victim's personal security to electronical identification. A criminology research professor Reyns (2013) therefore aimed to investigate how individuals online routine and identity theft victimisation is correlated by applying a routine activity approach to a non-physical proximity. By using data from the British Crime Survey, Reyns (2013)

examined participants online routine activities such as shopping and banking, perceived risk of victimization on identity theft and individual characteristics such as age and gender. The result showed that individuals that used Internet for banking or online messaging are more likely, about 50 per cent, to be victimized by identity theft compared to others. Related, individuals who downloaded and online shopped, also had an increased risk of victimization by about 30 per cent. When analysing personal characteristics, older persons, individuals with higher income and males where at higher risk of experience victimization. A conclusion drawn from this is that "although the routine activity approach was originally written to account for direct-contact offences, it appears that the perspective also has utility in explaining crimes at distance" (Reyns 2013, p. 219).

Previous Research

Cybercrime is a concept for all criminal offences perpetrated using Internet and information technology (Mehan 2014). The definition of this types of crime in cyberspace, has however been contentious where different typology has been used. Some researchers chose to describe cybercrime as digital technology crime or electronical crime due to the nature of using mobile phones or social media to commit such offences (Waller et al. 2015). However, there does not exist one single characteristic of these crimes, meaning, that cybercrime is committed at several online services and in different ways. Regardless of terminology used, cybercrime aim to encompasses all different types of criminal offences committed by using information technology and Internet (Mehan 2014).

Identity related Crimes

Within the concept of cybercrime lies identity related crimes. Identity related crimes occurs when a perpetrator unlawfully obtains another person's information without their knowledge or consent to commit other types of crimes such as fraud. The purpose for such behaviour is various such as economic gain, espionage or to posing as another individual. It can also be to use another person's identity to obtain government documents or benefits using the victim's identity. These crimes can be committed by a single individual or by criminal networks (Cassim 2015). In criminological research a commonly accepted definition of the problem evolving identity related crime does not exist, and therefore researchers use different terminology and the crime statistics on this area is distorting (Koops 2009). Identity related crimes has arisen from the use of electronic services partly provided by the banking sector. An electronical identification system is a recent development; however, bank identity is not a new phenomenon but has been used and formalised since the early 1960s were bank validated bank identity cards (Husz 2018). In research scientists often agree that electronical identification system is important for the online world and development of society. There is also an agreement that electronical identification give rise to identity-related crimes. However, what is still unknown is the range of crimes that can be included in the definition of identity related crimes and new crime types and methods continues to grow (Koops & Leenes 2006). It is also unknown how these definition of identity theft and identity fraud should be viewed legally and combated by the authorities and government. When comparing different official reports, it becomes difficult due to the existence of different definitions and on top of that, these definitions is rarely described. Due to the lack of common typology, combating the growth of identification related crimes risk to be unsuccessful (Koops 2009).

Modus Operandi

Perpetrators that commits identity related crimes, use different methods to obtain personal or financial information by electronical identification (Dobrinoiu 2014). Social engineering is one of the method used, where the perpetrator deceives or manipulate the victim by communication strategies. Here the perpetrator has a conversation with the victim directly by phone or by electronical mean of communication with aim to make the victim disclose data to the perpetrator or take actions in benefit for the perpetrator (ibid). Another common method is phishing, where the perpetrator focuses more on stealing personal identification for electronic payment. Often the perpetrator send their victims convincing e-mail message or hyperconnexion (links) to a fake website. The server is controlled by the perpetrator and the victim is then tricked into leaking personal data or other information used when making financial transactions or shopping online (ibid).

The Police Authority explained in a report 2017 that many perpetrators try to steal others BankID which can give these perpetrators financial benefits and possibility to access important and sensitive information such as making changes in public records, payments and pension savings (Polismyndigheten 2017). Identity related crimes using BankID may generate a large amount of money from many smaller criminal acts to make a big profit. Money that may be used to finance other criminal activities. Perpetrators can live in other countries and target Swedish citizens and vice versa, which is an example of how these crimes can occur across national borders (ibid).

The Swedish National Council for Crime Prevention (Brottsförebyggande rådet 2018) reports that fraud in general increases in today's society and that mainly because of that the use of Internet that has increased and the technical development contributes to opportunities for fraud online. Also, fraud committed online can target several people at the same time which also could explain why fraud committed via Internet is the crime type which increases the most today. The trend is nearly the same for both men and women, where men are a little overrepresented. The crime methods used are the ones that are most sensitive to criminal attacks. For example, under the 1980s check fraud was more common but when this payment tool become less common also did the crimes. Instead credit card fraud increased as this type of payment became more common. In 2000s fraud, and specifically fraud online, has increased significantly. There is an increase both in the self-report study Swedish Crime Survey (SCS 2017) and police reported crime statistics. However, the increase is higher regarding reported crimes compared to SCS that can be explained by SCS only measuring individuals and not companies and authorities' victimization regarding fraud (ibid).

Combat Crime

Cybercrimes are developing at the same rate as the Internet and it puts pressure on the legal system to develop laws adapted to these types of crimes. Identity theft is a challenging problem when it comes to the legal system and law enforcement (Cassim 2015). Moreover, policies to combat identity related crimes in an electronical aspect varies and may not always target the problem at its core (Koops 2009). Identity theft exists in a virtual world, therefore government and law enforcement agencies must work together with businesses and consumers in different jurisdictions and with a multi-disciplinary approach. There also has to be a legal perspective to improve collaboration between countries (Cassim 2015)

To combat identity related crimes, law enforcement agencies tries to advance technology by technical solutions in order to address vulnerabilities in computer system and enhance consumer awareness (Cassim 2015). Some steps that is recommended when it comes to combat identity related crimes are: raise businesses awareness, educate consumers about protecting their identity online, improve collaboration between countries and jurisdictions, improve collaboration between government and local banks, work together with identity theft victims to provide help and at last set a plan to prevent or minimise the harm regarding identity related crimes (ibid). Some researchers also sensitize that if the only focus is at criminalization, prevention of the crime may be forgotten. The focus must therefore also be on the enablers of these crimes, such as lack of security concerns and lack of public awareness (Koops 2009). However, if the security rises to high, consumers may also experience the technology device to complicated. There is videlicet a balance between enhanced security and user-friendliness. To overcome this problem, raising public awareness has instead been seen as a more effective method to overall fight identity related crimes (Ibid). One action the Police Authority in Sweden takes to reduce fraud, is to inform citizens about how they can stay safe online. Together with other European countries an information security month is held every October since 2012. Since more people use the network and meanwhile perpetrators are getting more effective in their actions to commit crimes increased knowledge in society regarding fraud is highly important (Polismyndigheten 2018).

Method and Ethics

This section that follows, will describe thesis procedure and which choices and delimitations that were made to increase replicability. Within research, replicability is important because for knowledge to be generated research must be both sincere and clearly described regarding the course of proceedings that lead up to the result (Forsman 1997). In this study interviews with representatives at banks and the Police Authority has been held in order to investigate cybercrimes against electronical identification by using BankID as the main case study and to also investigate how these authorities combat cyber financial crimes.

Planning for the Thesis

The purpose of the study was chosen due to that identity fraud is a crime category that increases most in society today and the course of action is to commonly target or use technology devices where these criminal acts can be carried out (Brottsförebyggande rådet 2019). When researching for previous studies, it was clear that the subject is fairly unexplored. Even though using several keywords and searching in different data bases only a limited amount of studies was found and those found were often recently published. In the thesis background a precedent of court were described to emphasise legislation on the topic. Thus, court cases are official but involves sensitive information, all material has been carefully treated during the project, where only the student in charge have had access to the material. To investigate the slightly unexplored topic for this study, a choice to carry out interviews with different bank agencies was made to answer what safety risks there are using electronical identification, as BankID. Likewise, interviews was chosen as method to answer how the Police Authority and Swedish Economic Crime Authority in Sweden combat cybercrimes in this area.

Previous studies have used different methods to investigate the risk with electronical identification. A common method was to qualitative describe how authorities are combating these crimes and to describe the typology by comparing crime modus (Cassim 2015, Koops 2009). Another more rare method among the previous studies was to use quantitative data. One such study was Kranenbarg et al. (2017) that used a sample of adult suspects of cybercrime. However, because of the topic being rare in criminological research and due to the Swedish legislation being recently updated in 2016 with the unlawful identity use (Law 2016:485) and EU-directives, a quantitative method was disregarded. Crime statistics was seen too difficult to analyse due to law changes that changes how the statistics is measured and due to electronical identification being a quite new approach for society. The qualitative approach is on the other hand more useful when wanting to learn more about a topic. In consideration of this, the interviews are of a qualitative approach which is an advantage when striving to gain more knowledge about a diverse and complexed phenomenon (Bryman 2008).

Ethics

When the project plan for the thesis were completed, work began on an ethic application. In order to maintain good ethics, the researcher can let ethical committees consisting of independent representatives take a position on the research project (Forsman 1997). In this case, the purpose and approach of the study has been ethically tried by the ethics council at Malmö university, and granted according to HS2019/löp.nr. 43, stated 2019-03-01 (Appendix 1).

When conducting research, different factors should be considered. Research project should generate new knowledge, but on the other hand also protect those who participate in the study (Vetenskapsrådet 2011). To maintain a balance between ethical requirements, primary ethical criteria in the publication Economic and Social Research Council (ESRC 2015) has been followed. In accordance with the information and consent requirement, the researcher should keep the participants well informed about the purpose, method and use of study and that all participation is voluntary and can be ended at any point (Bryman 2008). The information to the participants should also be truthful and well conducted so that it is easy for the participants to understand the aim of study (Forsman 1997). In order to enforce these requirements, each respondent from the agencies was given an information letter of the purpose and method of the study and was thereafter asked to give a consent to be part of the interview (see Appendix 2).

Furthermore, a usage requirement was considered concerning that all material collected only should be used for the specific research purpose (Bryman 2008). In this case, it was made clear that the study is a student thesis aiming to investigate BankID safety risks and prevention. Another ethical aspect considered was the confidentiality requirement, stating that all personal data of participants should be treated with carefulness so that participants are protected from unauthorized (Jacobsen 2007). As the study address agencies, the principal at each agency acts in their role as an official. However, in interviews sensitive information or personal opinions can be seen through and therefore, only relevant findings regarding the topic of thesis have been described in the result. During the conduct of the interviews, ethics were considered by the fact that the student in charge strived to not ask leading or unambiguous questions, because the researcher should not use the research method to get the answers desired (Forsman 1997).

The Study's Approach

After the ethical application was approved, an interview plan was made were different questions was created (see Appendix 3 & 4). When the interview plan was done and interviews held, the reporting of interviews began, which was concluded by a discussion.

Interview Questions

The design of interview was of a semi-structured approach to investigate certain questions and to gain validity by including open-ended questions that could contribute to a nuanced and deeper knowledge (Bryman 2008). The questions were created given that they should not be unclear nor leading, that could mislead the respondent in a certain direction. In every interview among the banks the same questions was asked to create a comparative design regarding what safety risks there are using BankID. Regarding the interviews with the Police Authority other questions were asked in order to answer how the Police Authority and Swedish Economic Crime Authority combat cybercrimes in this area. In some cases, follow up questions was asked or the question were asked in another order to generate more in deep answers. It was important not be too tied to the interview plan because it could disadvantageous prevent new aspects to arise (Bryman 2008). The interviews began with a repeat of purpose and that all participation was voluntary. The interviews ended with an explanation of how the result would be complied. Each interview lasted for approximately one hour to 45 minutes.

Sample

The different bank agencies that were asked to be a part of the thesis was all eleven banks that provides BankID. Three major banks in Sweden namely Handelsbanken, Nordea and Swedbank agreed to participate. Four banks (SEB, Forex Bank, Scandia Banken, Länsförsäkringar) declined most due to security policy or either that they did not have time to participate and four banks (ICA-Banken, Sparbanken, Ålandsbanken, Danske Bank) did not respond despite several remainders via telephone and e-mail. Me as conductor of study called each bank with information about the study and its method and with question if they would like to participate. To also clarify the thesis an e-mail was sent to the agencies with description of aim, method and ethical criteria that the study considers. To compensate for the banks that did not participate, the BankID organisations was asked if they could participate with their perspective which they approved, and their answer can hopefully represent an overall view of what safety risks there are using electronical identification, as BankID. To also investigate the second research question in how these crimes can be prevented or investigated, me as a conductor interviewed a representative at the Police Authority. The Swedish Economic Crime Authority were also asked to participate, however with several attempts to ask for participations via telephone and e-mail I got different responses. On one hand, they responded that they had difficulties to find a representative that could answer my question. I also got the answer that they could not participate due to security policy but that I could try to another department at the authority. After I tried that, there were no response from the authority despite several attempts. Overall, the three banks, together with the Police Authority and the organisation of BankID expressed that they wanted to participate in an interview. All interviews were booked on separately dates and held either by telephone (due to geographical difficulties) or at meetings in Mars to April 2019.

Transcribing Interviews into a Result

After each interview, the recording and notes was transcribed to a result

containing the main findings. The interviews were held in Swedish though the findings have been translated into English. The translation and implementation of the analyses has thus been carried out carefully through a thematic analysis, with attempt to be objective in the interpretations. The result is written through the respondents' words and point of view and written in paragraphs that represents the main important topics or emphases that the respondents made. Due to that qualitative data often generate a wider range of material, it can be difficult to delimit the findings (Malterud 2014). To delimit the material but avoid missing important information, the transcribed text was read through several times. The result shall further reflect the different agencies perspective of the problem, however in some cases the findings may possibly represent the individual respondent (Gadd et al. 2012). After conducting the result, a discussion was written together with a suitable perspective of theory.

Result

The result presents the bank representatives from Handelsbanken[1], Swedbank[2] and Nordea[3] and their perspective of BankID and security. Thereafter an overview of the BankID organisation's[4] perspective is described as well as the Police Authority's[5] perception of how crimes regarding BankID are prevented.

BankID and Security Risks

All the banks explain that the greatest security risk regarding BankID today is not the technology nor security-related functions but instead the users or customers. The product managers at the banks explained that no perpetrator has been nearby to hack BankID and that we therefore do not have to worry about that today. However, it can never be said that it always will be 100 per cent secure and perpetrators use different methods to access another individuals BankID. All participants of the banks explained that common modus for illegally access others BankID is through Facebook-fraud, social media or telephone scams. Regarding Facebook-fraud, the participants explained that it has been common modus for the perpetrator to hack the victims Facebook and to thereafter start to contact the victim's friends. The perpetrator often read previous messengers and look on photos or life events to pretend to be the victim he or she has hacked. When the perpetrator then chat with the victim's friends, the perpetrator become more reliable and could thereafter try to trick the victims friend into lending money to the perpetrator because they thought that they chat with their friend.

Regarding telephone scams, common modus is for the perpetrator to call people and pretend to represent the bank. This modus is called Voice phishing and the perpetrator can for example tell the victim that someone is transferring money from the victims account and ask if the victim want to stop the transaction. If the victim gets that message and believe in it then it is a natural reaction for the victim to do almost anything and then it is easy to be deceived. All participants comment that this is a big security risk. Two of the representatives, Nordea and Handelsbanken, also mentioned the risk regarding illegally downloading another

[1] As per personal communication with Handelsbanken representative P.G, 2019-03-21
[2] As per personal communication with Swedbank representative P.W; 2019-03-27
[3] As per personal communication with Nordea representative N.W; 2019-03-28
[4] As per personal communication with BankID Organisation representative C.P; 2019-04-10
[5] As per personal communication with Polismyndigheten representative J.O; 2019-04-03

person's BankID. This could happen for example if the perpetrator falsifies the victims ID and enters a bank office with a request for a bank-box to download a BankID. The same result can be obtained if the perpetrator trick the victim into giving up the code to the bank-box. It is a one-time code that the perpetrator can use to download a BankID in the victim's name without the victim knowing it. Regarding identity theft Nordea also comment on the sensitivity of stealing personal information, that if the perpetrator has come across a customer's BankID then all electronical information is wide open to steal, which can result in great damage for the victim. Swedbank mentioned that getting a hold of someone else's personal information is quite simple in Sweden today and that the deceivers constantly change the crime approach depending on what is most successful.

Past Safety Risks and Preventative Activities

All participants mentioned that the banks often do not talk publicly about preventative activities due to its sensitive nature. Swedbank mentioned a focus for BankID today, namely to "*making the product more secure and harder to use when attempting fraud but also to develop user-friendly functions such as biometrics (FaceID and fingerprints)*". For example, if the customer is sitting on the bus there is a risk that the perpetrator look over the victims shoulder too see the victim's code. However new developments are targeting this modus such as fingerprints and FaceID. QR-codes was one development with BankID that all banks mentioned. Handelsbanken mentioned that "*the latest change of QR-code has been very effective against a certain type of fraud for example Voice phishing (Vishing)*". This development is effective in cases where the targeted computer and phone are in different places. Then one need the QR-code to for example downloading a new BankID which has prevented many criminal acts.

Regarding if BankID is a secure product on any devise, both BankID on file and mobile BankID, the general answer from the banks was that the security is equivalent where every device is safe but there can also be different opinions. A particular unit may for example be more exposed depending on what the fraudsters are focusing on. However, it is not the technical solution that one is interested in, but instead to trick the individual into giving up the code. All banks mentioned that elder people often are targeted for fraud regarding BankID. Perpetrators often figurate as goalkeepers and a risk groups is younger people or socially excluded individuals who lend their account for money transactions that they think is harmless. All banks mentioned that it is difficult to predict what the future will hold regarding IT-Security. Swedbank explained that "*the difficult thing is to constantly adapt the development to the fraudsters new approaches*".

Cooperation with the Police Authority and other Banks

All banks mentioned that they cooperate with the Police Authority and other banks as well. Handelsbanken explained that they cooperate with the Police Authority and help to detect crimes and find the perpetrators. Swedbank explained that "*they and their BankID supplier cooperate with the Police Authority and Swedish Economic Crime Authority and they contribute to police investigations*". Nordea also discussed that they have a cooperation with the Police Authority and Swedish Economic Crime Authority. If the customer is exposed to fraud regardless of whether it succeeds or not, a police report is filled and the police and Nordea exchange information. Regarding the Swedish Economic Crime Authority often major economic crime is discussed. The banks also cooperate with the police outside fraud cases to spread information about BankID security.

The BankID Organisation's Perspective

The BankID organisation explained that BankID is an e-ID that enables companies, banks, organizations and authorities to identify and enter into agreements with private individuals on the Internet. Their most important task is to ensure that BankID is a secure e-ID. They work continuously with safety and maintenance work so that their users feel safe when using BankID. In the autumn of 2018, they launched QR-code in the Mobile BankID app. An additional step to strengthen the safety use of BankID with the reading of QR-code so the user can confirm the physical proximity between his computer and mobile phone. Most network fraud occurs today when the fraudsters call and trick the user into entering their BankID code several times, called Vishing fraud. However, the BankID organisation stated that there are no risks with using Mobile BankID if the customer follows safety use to, "*always and carefully read the text shown in the BankID app, never leave the code to anyone else, never use the BankID at the request of another person, and if you suspect that you are exposed to fraud, you should block your BankID, contact your bank and make a police report*".

How Police Authority Combat Cybercrime regarding BankID

The police representative explained that fraud regarding BankID is investigated as all other crimes within the police. However, it has in general a lower priority within the authority because the legislators consider that it concerns money but that idea is outdated as this is a mean of financing other crime such as terrorism, human trafficking or drugs and that must be taken into consideration. It also targets the elderly in society that takes physical and mental damage. Goalkeepers are often used such as younger people and Vishing fraud attracts organizations to profit from causing others to commit fraud. It is a more serious crime than one can imagine. However, the police do not have enough resources to target these crimes. The police "*estimates that they can handle 5 per cent of the reported offenses*" because they do not have time given the proportion of police investigators.

The police cooperate with the BankID organisation itself and with the banks all the time. They also have ongoing discussion with companies such as American express, Moneygram, and Western union, since the entire digitization goes towards electronic money but it is also something the market requests. However, all technical solutions must be safe and that development can never stop in the technological products such as BankID. Here, the police help with information or cooperation to always secure technological products. The perpetrators do not only act in one country, they act online and the police cannot investigate if they do not receive information from other countries. Moreover, other things can also disturb, for example how tele-companies chooses to interpret EU-directives around the possibility of saving information, IP tracking etc. The consequence is that the police cannot track criminals online where the digital information is sometimes the only evidence. The perpetrators get new digital tools hide behind and the police have more difficulty to track them, "*the combination is not successful*".

Regarding a legal perspective, the law does not always keep up with the technology development but the police tries to inform about that as well. The aim when raising safety is to make it as difficult as possible to misuse the product. The product BankID itself, is safe but the security risk is the user who can be manipulate to use the BankID code incorrectly, called social engaging. However, what has been seen recently in the police operation 'Dimma' is that the modus operandi where perpetrators called the victim to trick the victim into getting

BankID codes has decreased due to the launch of QR-codes which requires the perpetrator to have the victims mobile phone in the physical presence. On the other hand, regardless of how safe the BankID solution is, perpetrators can induce people to make mistakes and it is the back side of the digitization's advance. The modus also changes over times regarding fraud against BankID so it is an ongoing project for the police to combat these crimes. The perpetrators will never stop trying to commit fraud and nothing is 100 per cent secure. The perpetrators also make judgements regarding how much time they should spend finding a way to commit fraud in relation to how much money they can earn. The easiest method is chosen, such as to trick people rather than trying to hack BankID. Regarding risk of stealing the victim's electronical identification for identity theft, Sweden has a publicity principle but in contrary all digitization causes different types of danger.

Discussion

The discussion that follows, regards the result and method of the thesis. Different perspectives are elucidated and discussed based on what has been identified and presented. The discussion ends with a conclusion.

Method Discussion

The method discussion highlights the validity of the study and future research. Thereafter follows a discussion regarding the reliability.

Validity

This thesis is built upon a qualitative approach to investigate what the safety risks are using the electronical identification BankID and how authorities combat crimes regarding these electronical identifications. Due to the difficulty of finding previous studies with similar research question, a quantitative approach was not found appropriate. Research from other countries is also rare because BankID is a product used in Sweden even though electronical identification systems exists in other countries. Using a quantitative approach was also seen difficult due to the Swedish legislation being recently updated which affects crime statistics and makes it difficult to analyse longitudinal. Electronical identification is also a quite new approach for the society and therefore a chose to use a qualitative approach was made because this method is useful when striving to gain more knowledge about a diverse and complexed phenomenon (Bryman 2008). On the other hand, for the future it would be beneficial to study the topic using other research methods to illustrate the research questions. Despite the benefit using a qualitative method to illustrate a new topic, the difficulty to find a suitable method can still be seen through. Due to the subject being rather unexplored within criminological research no guideline nor recommendations from other researcher could be found. This problem can for example be seen regarding the second research question surrounding the police authority and Swedish Economic Crime Authority. The plan was to illustrate the authorities in Sweden who work with financial crime, since BankID is mainly used for economic purposes. However, it was difficult to find a representative at Swedish Economic Crime Authority and this could possibly have been avoided if there were other studies to draw lessons from.

When it comes to the interviews an interview plan was made with several open based questions to create a broader perspective of the topic. At the same time, the qualitative approach also generally generates a large material, so to keep the

theses concrete and not too long, a discourse analysis was made where the material was delimited and the processing systematically performed, to identify different emphasis and subthemes. To increase the validity, the approach and shortcomings should also be clearly stated, which has been an aim in this thesis (Malterud 2014). Something more difficult to prevent was that the method of interviews was time consuming. Requests of participation was sent to all banks that are part of the BankID cooperation, but many repeated attempts were required both by mail and phone to both get a hold of right representative and to get an answer on whether they could and wanted to participate in the study. It would have been beneficial to interview several banks as well as the Swedish Economic Crime Authority, but some banks chose not to participate and many answers were not materialized. In research based on active communication with participants, it is known that it may take time and repeated attempts to get answers (Bryman 2008), and in this case, it resulted in all the banks and authorities surveyed not being able to be represented.

When it comes to the external validity it defines how well the results can be generalized to a larger population (Jacobsen 2007). In this case, the result is based on Swedish authorities' and banks' perspective regarding issues of electronical identification and consequently is foremost applicable in Sweden. Regarding interviews a problem is that sensitive information or personal opinions can be seen through. Therefore, when transcribing only relevant findings from the questions has been described in the result.

Reliability

A higher reliability can be achieved if the study approach is presented in a clear and comprehensive way. The purpose of replicability is that others should be able to replicate the study and obtain the same result (Jacobsen 2007). To maintain this requirement, it has been important in the thesis to describe the method and its deficiencies pervading, so that the result not become misjudged nor misinterpreted. Hence, reliability should be good in this regard. Regarding the interviews, all participants asked to participate in the thesis has been mentioned in the method and the interview questions are also described. However due to that interviews are created in a personal communication replicability and obtaining the same answers may be difficult, due to that interviews are conducted at a certain point in time, at a certain place and with a certain selection of respondents and their agencies (Bryman 2008). To prevent this problem, the respondents in this thesis are the official representatives of the respective organizations. Also, the bank officials have responded similarly and raised similar factors. Even a cease in the result could be felt, meaning the result might not have been affected if another bank had been interviewed. However, it is difficult to estimate if the result could be different if more participants were represented or if the study is replicated. Furthermore, the thematic analysis does not have as clear guidelines to systemize the result and because the interviews generate a wider range of material, some findings had to be reduced from the final report (Malterud 2014). The interviews were also held in Swedish though the findings have been translated into English. The translation and implementation of the analyses has thus been carried out carefully, and read through several times. In summary, the method has been throughout described so that it can be replicated.

Result Discussion

This result discussion reflects to the research questions and highlights the main

findings relevant for the research questions. Important is that due to that the Swedish Economic Crime Authority is not represented in this thesis, the second research question can partly not be answered. Therefore, only the Police Authority's perspective will be discussed.

Electronical Identity Related Crimes and Prior Research

When it comes to criminological theory, two theories have been earlier discussed, white-collar crime and the routine activity theory. White-collar crime has been discussed as quite fair when it comes to identity thefts where perpetrators often have different backgrounds and a common motive for committing identity theft is a need for quick money. Often, these perpetrators are targeting information or victims that they can access or approach more easily, or they might seek vulnerabilities in the networks that provides sensitive information (Copes & Vieraities 2007). Another criminological theory that has been applied on identity theft, is the routine activity theory, however with a non-physical proximity (Reyns 2013). Peoples routine activities can matter when it comes to identity thefts, where people who use Internet for banking or online shop, are at an increased risk of victimization. Also, characteristics matters where elder persons and males seems to be at greater risk of victimization (ibid). When it comes to criminological theory, there is difficult to discuss the theories applied to identity thefts, white-collar crime and the routine activity theory, on the result of this thesis. This is because the topic within criminological research is fairly new and it can then be skewed to base this result on a limited finding of research articles. Furthermore, some research findings, for example Copes and Vieraities (2007), stating that the perpetrators often want to earn quick money and that elderly people often are victimized seem to be accurate also for the findings in this thesis. However, there is little knowledge regarding the perpetrators behind the goalkeepers. There can also be hidden statistics regarding the tendency to report crime, for example, are elderly people more vulnerable, or does there exist a tendency for people to not report crime.

Regarding the second research question, the Police Authority has published some information about how they work to combat identity related crimes. Two methods described in the previous research has also been highlighted in this thesis. Firstly, law enforcement agencies try to advance technology by technical solutions to address vulnerabilities in computer system (Cassim 2015). Technical solution has in this thesis been a major topic for both the banks and the Police Authority, for example the discussion regarding QR-codes. Another method mentioned in previous research in order to combat these crimes, that also has been highlighted in this thesis result, is the importance of raising public awareness (Cassim 2015). Both the Police Authority and the banks implies the importance to inform people about the risk of electronical identity related crimes and how a customer can be protected. When it comes to differences regarding results found in this thesis and results from previous research, as mentioned above it is difficult to detect any major differences due to the topic being fairly new and unexplored. More research is needed in order to deepen future discussion regarding identity related crimes.

BankID and Safety Risks

The main findings regarding BankID and safety risks, the first research question, is that all participants stated that the greatest security risk regarding BankID today is not the technology or security-related functions but instead the users or customers. The product managers at the banks, the Police Authority and the

BankID organisation explained that no perpetrator has been nearby to hack BankID and that we therefore do not have to worry about that today. Instead, perpetrators use different methods to access another individuals BankID. All participants of the banks explained that common modus for illegally access others BankID is through Facebook-fraud, social media or telephone scams. The banks also comment on the sensitivity of stealing personal information, that if the perpetrator has come across a customer's BankID then all information tied to the electronical identification is wide open to steal, which can result in great damage for the victim. The Police Authority discussed more than the banks that the problem with fraud regarding BankID is not as much of a problem than it was last year in 2018 due to the launch of QR-code. However, the police also discussed that fraud takes new modus and changes over time. All banks mentioned that they cooperate with the Police Authority and other banks as well.

How the Police Authority Combat Crimes targeting Electronical Identification

Findings from the police illustrates how cybercrime surrounding identity related crimes is combated, to answer the second research question. Crime regarding BankID is investigated as all other crimes within the police. However, it has in general a lower priority within the authority because the legislators consider it a concern of money, but that idea is outdated as this is a mean of financing other crimes and it also targets the elder in society. The police cooperate with the BankID organisation itself and with the banks. They also have ongoing discussion with companies, since the entire digitization goes towards electronic money. The police also help with information about secure technological products and trice to inform customers about safety and risks regarding BankID. The perpetrators come up with different methods to commit fraud against BankID and they get new digital tools to use anonymously, so it is an ongoing and difficult project for the police to combat these crimes.

Conclusion

To summarise, when it comes to criminological theory, there is difficult to discuss the theories applied to identity thefts, white-collar crime and the routine activity theory, on the result of this thesis. This is because the topic within criminological research is fairly new and it can then be skewed to base this result on a limited finding of research articles. Regarding the first research question, the thesis result show that it is mainly the customer, not product or security-related functions, that are the main safety risk surrounding electronical identification of BankID and perpetrators use different modus to access another individuals BankID. Regarding the second research question, the result is partly defective, due to the Swedish Economic Crime Authority not being represented in this thesis. The second research question can partly not be answered and the focus has therefore been to investigate the Police Authority’s perspective. The police investigate fraud regarding BankID as all other crimes but it has in general a lower priority within the authority. The police cooperate with the BankID organisation itself and with the banks to keep the product secure. They also have ongoing discussion with companies and helps with informing customers about safety and risks regarding BankID. Taken together, when it comes to differences regarding results found in this thesis and results from previous research, as mentioned, it is difficult to detect any major differences due to the topic being fairly new and unexplored. More research is needed to deepen future discussion regarding identity related crimes surrounding BankID and how authorities work to combat these crimes.

References

Adams J, (2014) Norway's MeaWallet to Use Sweden's BankID Security Standard. *Payments Source NewsBank*, 1-3.

BankID, (2018) Statistik BankID – användning och innehav – fördjupning. > https://www.bankid.com/assets/bankid/stats/2018/statistik-2018-12.pdf< PDF (2019-04-01)

BankID, (2019) *Detta är BankID.* >https://www.bankid.com/om-bankid/detta-ar-bankid> HTML (2019-02-01)

Brenner S W, (2012) *Cybercrime and the Law*. Boston, Northwestern University Press.

Brottsbalk (1962:700)

Brottsförebyggande rådet, (2018) Kortanalys 5/2018, Kortanalys om brottsutvecklingen. *Brottsförebyggande rådet*, Stockholm, 1-33.

Brottsförebyggande rådet, (2019) Kriminalstatistik 2018 Anmälda brott slutlig statistik. *Brottsförebyggande rådet enheten för rättsstatistik*, Stockholm, 1-58.

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

Cassim F, (2015) Protecting Personal Information in the Era of Identity Theft: Just How Safe is Our Personal Information from Identity Thieves? Potchefstroom Electronic Law Journal, 18 (2), 1-43.

Cohen L E, Felson M, (1979) Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*, 588-608.

Copes H, Vieraities L, (2007) Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk. *University of Alabama at Birmingham, Department of Justice Sciences*, 1-87.

Dobrinoiu M, (2014) ID-Theft in Cyberspace. *Faculty of Law Nicolae Titulescu University of Buchares: Challenges of the Knowledge Society*, 4 (1), 5-8.

EU nr 910/2014. Europaparlamentet och rådets förordning.

ESCR, (2015) *ESRC Framework for research ethics* >http://www.esrc.ac.uk/files/funding/guidance-for-applicants/esrc-framework-for-research-ethics-2015/<PDF (2019-04-10)

Felson M, Boba R, (2010) *Crime and everyday life. Fourth Edition*. Thousand Oaks: SAGE publications.

Forsman B, (1997) *Forskningsetik – En introduktion*. Stockholm, Studentlitteratur

Gadd D, Karstedt S, Messner S F, (2012) *The SAGE Handbook of Criminological Research Methods*. London: SAGE

Husz O, (2018) Bank Identity: Banks, ID Cards, and the Emergence of a Financial Identification Society in Sweden, *Enterprise & Society*: *Cambridge University Press*, 19 (2), 391-429.

Jacobsen D I, (2007) *Förståelse, beskrivning och förklaring: introduktion till samhällsvetenskaplig metod för hälsovård och socialt arbete*. Lund: Studentlitteratur.

Koops B J, Leenes R E, (2006) 'ID theft, ID fraud and/or ID-related crime. Definitions matter'. *Datenschutz und Datensicherheit*, 30 (9), 553–556.

Koops B J, Leenes R E, Meints M, Van der Meulen N, Jaquet-Chiffelle D O, (2009) A Typology of Identity-Related Crime: Conceptual, Technical, and Legal Issues. *Information, Communication & Society*, 12 (1), 1-24.

Kranenbarg M W, Holt T J, Van Gelder J L, (2019) Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. *Deviant Behaviour*, 40(1), 40-45.

Malterud K, (2014) *Kvalitativa metoder i medicinsk forskning*. Lund: Studentlitteratur.

Mehan J E, (2014) *CyberWar, CyberTerror, CyberCrime and CyberActivism: An In-depth Guide to the Role of Standards in Cybersecurity Environment*. United Kingdom, IT Governance Publishing.

Moskowitz S, (2017) *Cybercrime and Business: Strategies for Global Corporate Security*. Minnesota, Elsevier Science.

NJA 2017 s.1105

Piquero Leeper N, (2018) White-Collar Crime is Crime, Victims Hurt Just the Same. American Society of Criminology. *Criminology and Public Policy*, 17. (3), 595-600.

Polismyndigheten, (2017) Polisens rapport om allvarlig och organiserad brottslighet 2017. *Polismyndigheten: Nationella operativa avdelningen*, Stockholm, 1-18.

Polismyndigheten, (2018) Stor europeisk informationsinsats för att minska bedrägerier. >https://polisen.se< (2019-04-05)

Reyns B W, (2013) Online Routines and Indetity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of research in Crime and Delinquency, SAGE: Publications Inc,* 50 (2), 216-238.

Sutherland E H, (1940) White-Collar Criminality. *American Sociological Review: American Sociological Association*. 5 (1), 1-12.

Sveriges Riksdag, (2016) Lag (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. >http://www.riksdagen.se<HTML (2019-04-02)

Vetenskapsrådet, (2011) *God forskningssed*. Stockholm, Vetenskapsrådet

Waller L G, Bailey C, Johnson S, (2015) *Fear of Cybercrime, Lessons for the Global E-banking Sector*. Miami, Ian Randle Publisher Kingston.

Appendices

Appendix 1. Ethical Approval, Ethic Council at Malmö University

HS2019/löp.nr. 43, stated 2019-03-01

Malmö universitet / Fakulteten för Hälsa och samhälle
Etikrådet
Adm sekreterare Ewa Sortberg Bassmann

Utlåtande

2019-03-01 **HS2019 löp nr 43**

Projekt: Cybercrime using Electronical identification, what are the danger for Criminality?

Student: Eleonor Brandt Hjertstedt

Handledare: Robert Svensson

Föredragande: Åsa Alftberg

Etikrådets utlåtande:

Ansökan gäller en studie som syftar till att undersöka synen på IT-brottslighet gällande elektronisk identifikation/BankID med utgångspunkt i verksamheter såsom banker, polismyndigheten och ekobrottsmyndigheten.

Etikrådet vid HS prövar sådana ansökningar som omfattas av 3§ eller 4§ lagen om etikprövning. Där ingår exempelvis studier som innehåller känsliga personuppgifter, personuppgifter om lagöverträdelser eller som innebär en uppenbar risk att skada forskningsperson psykiskt eller fysiskt. Ansökan är inte av sådant slag att Etikrådet ska pröva den. Eftersom den har kommit rådet tillhanda lämnar vi ändå några rekommendationer som vi hoppas kan vara till gagn för det fortsatta arbetet:

- Samtycke kan inhämtas antingen skriftligt eller muntligt. Vid muntligt samtycke ska detta dokumenteras, t ex spelas in. I denna studiedesign med telefonintervjuer kan muntligt samtycke vara att föredra.
- Data ska behandlas konfidentiellt och förvaras på sådan sätt att ingen obehörig kan ta del av det.

För Etikrådet vid Fakulteten för hälsa och samhälle, Malmö universitet.
Åsa Alftberg

Postadress	Besöksadress	Tel	Fax	Internet	E-post
Malmö universitet Fakulteten för hälsa och samhälle 205 06 Malmö	Malmö sjukhusområde Jan Waldenströms g 25	040-665 74 54	040-665 81 00	www.mah.se	etikradet@mah.se

Appendix 2. Information Letter

MALMÖ UNIVERSITET **Informationsbrev** **Bilaga 1**

Projektets titel: **Cybercrime using Electronical Identification, what are the Danger for Criminality?**	**Datum: 2019-02-15**
Studieansvarig: Eleonor Brandt Hjertstedt **Din E-post:** [redacted]	**Studerar vid Malmö universitet, Fakulteten vid hälsa och samhälle, 205 06 Malmö, Tfn 040- 6657000** **Utbildning: Matser of Criminology** **Nivå: Master Degree Project**

Hej!

Mitt namn är Eleonor och jag är student på mastersprogrammet i kriminologi vid Malmö universitet. Jag skriver min masteruppsats med titel "*Cybercrimes using Electronical Identification, what are the Danger for Criminality*".

Uppsatsens övergripande syfte är således att beskriva och diskutera IT-brottslighet gällande elektronisk identifikation. Detta kommer att göras genom att undersöka hur banker (Swedbank, Nordea, SEB och Handelsbanken) samt Polismyndigheten och Ekobrottsmyndigheten i Sverige ser på IT-brottslighet kopplat till BankID. Riskerna för BankID kommer belysas samt hur man arbetar för att förbättra IT-säkerhet och förebygga samt upptäcka brott kopplat till användning av BankID.

Ni tillfrågas härmed om att vara med i en intervju som kommer bestå utav öppna frågor med temat BankID och säkerhet. Ni kommer ha möjlighet att besvara frågorna med egna ord och det är helt frivilligt att delta i intervjun. Det går även bra att välja ut de frågor som ni vill svara på om det är så att ni vill delta i intervjun men ej svara på samtliga frågor. Alla ni tillfrågade kommer att få besvara liknande frågor så att det finns möjlighet att analysera likheter och skillnader i hur banker samt myndigheter ser på BankID och säkerhet.

Medverkan i denna uppsats är helt frivilligt och *Ni* som deltar kan när som helst avbryta ert deltagande utan närmare motivering genom att meddela mig som studieansvarig eller helt avstå från att delta. Rapporteringen av resultatet sker sedan i form av en examensuppsats vid Malmö universitet och i uppsatsen kommer inga namn figurera utan att samtycke ges (utan endast bankens/myndighetens namn i så fall). Masteruppsatsen kommer att publiceras på Malmö universitet databas MUEP i juni 2019.

Härmed tillfrågas Du om deltagande i studien

Appendix 3. Interview Questions: Banks and BankID Organisation

- Vilka är de största säkerhetsriskerna med BankID?
- Vilka faror finns det gällande BankID och risk för bedrägeri?
- Vilka faror finns det gällande BankID och risk för att stjäla information eller personuppgifter?
- Hur har eventuella säkerhetsbrister sett ut?
- Vad har ni fått för respons gällande användning av BankID?
- Vad har ni gjort för förändringar gällande BankID?
- Vad ser ni för resultat av de eventuella förändringarna?
- Vad vill ni göra för förändringar framöver?
- Ser säkerheten olika ut beroende på vilken enhet man använder BankID?
- Samarbetar ni med Polismyndigheten eller Ekobrottsmyndigheten när det kommer till BankID?
- Vad innebär det samarbetet i så fall?
- Samarbetar ni med andra banker gällande BankID och i så fall hur?
- Hur ser ni på framtiden gällande It säkerhet?
- Hur ser ni på svensk lag gällande risker med elektronisk identifikation?
- Har ni någon uppfattning om vilka de ”typiska” gärningspersonerna eller brottsoffer som finns gällande brott kopplat till BankID?
- Hur ser det ut i andra länder gällande säkerhetsrisker med elektronisk identifikation?
- Har ni något ytterligare ni vill tillägga?

//English translation//

- *What are the biggest security risks with BankID?*
- *What are the current risks regarding BankID and risk of fraud?*
- *What are the danger for BankID and the risk of stealing information or personal information?*
- *How have any security deficiencies looked like?*
- *What response have you received regarding the use of BankID?*
- *What changes has been done regarding BankID?*
- *What results do you see of the possible changes?*
- *What future changes do want to perform?*
- *Does the security look different depending on which device BankID is used?*
- *Do you cooperate with the Police Authority or Swedish Economic Crime Authority and how do you cooperate when it comes to BankID?*
- *Do you cooperate with other banks regarding BankID and if so, how?*
- *How do you view the future regarding IT security?*
- *How do you view Swedish law regarding risks with electronic identification?*
- *Do you have any idea of what the "typical" perpetrators or victims there are when it comes to crime related to BankID?*
- *What does it look like in other countries regarding security risks with electronic identification?*
- *Do you have anything else you would like to add?*

Appendix 4. Interview Questions: Police Authority

- Vad ser ni för säkerhetsrisker gällande BankID och bedrägerier?
- Vad ser ni för säkerhetsrisker gällande BankID och att ”stjäla" annans personuppgifter eller information?
- Har ni någon uppfattning om vilka de ”typiska" gärningspersonen eller brottsoffer som finns gällande brott kopplat till BankID?
- Samarbetar ni med banker gällande säkerheten kring BankID och i så fall hur?
- Hur arbetar ni när det kommer till att förebygga och bekämpa brott kopplat till elektronisk identifikation såsom BankID?
- Hur ser ni på svensk lag gällande säkerhet kopplat till elektronisk identifikation?
- Hur ser utvecklingen ut gällande BankID och annan elektronisk identifikation?
- Hur arbetar ni med IT-säkerhet överlag?
- Hur ser det ut i andra länder gällande säkerhetsrisker med elektronisk identifikation?
- Har ni något ytterligare som ni vill tillägga?

//*English translation*//

- *What security risks are there regarding BankID and fraud?*
- *What security risks are there regarding BankID and to "steal" someone else's personal information?*
- *Do you have any idea of what the "typical" perpetrators or victims there are of crime related to BankID?*
- *Do you collaborate with banks regarding the security of BankID and if so, how?*
- *How do you work when it comes to preventing and combating crime linked to electronic identification such as BankID?*
- *How do you view Swedish law regarding security linked to electronic identification?*
- *What is the trend in terms of BankID and other electronic identification?*
- *How do you work with IT security overall?*
- *What does it look like in other countries regarding security risks with electronic identification?*
- *Do you have anything further that you would like to add?*