

Philip Johannes Brugmans Nyblom

Risk perception of identity theft in social media

Social media ID theft risk perception

Master's thesis in Master in information security

Supervisor: Gaute Wangen

June 2020

Philip Johannes Brugmans Nyblom

Risk perception of identity theft in social media

Social media ID theft risk perception

Master's thesis in Master in information security
Supervisor: Gaute Wangen
June 2020

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology



Abstract

Risk is something that we all concern ourselves with, risk is a combined measure of the probability and the consequence of something happening. How people perceive risk connects to their personal opinion on how risky doing something is. There are multiple possible risky behaviours on social media, and some of the things we post there might assist an attacker in performing identity theft. With social media being a new medium, there is a difference between how people use, and perceive risk. A compromised social media account gives an attacker the trust of the accounts of followers/friends. In this thesis, I show that attackers usually try to exploit accounts to use them for spam or phishing or to use saved credit cards associated with the account to buy ads. I also show what people believe that their accounts can be used for by an attacker. The thesis shows that people are very different in how they perceive risk, there are some trends regarding age and gender, with the older generation perceiving higher risks and women perceiving debate participation as riskier than males. My results demonstrate that we do not have a unified perception of risk on social media and that public discourse can stifle groups who perceive risk as higher than others. It also shows that an attacker usually wants to exploit trust with accounts; one can use this to manipulate public opinion.

Sammendrag

Risiko er noe vi alle er opptatt av, risiko er sammenhengen mellom sannsynlighet og konsekvens for at noe skjer. Hvordan folk oppfatter risiko kobles til deres personlige mening om hvor risikabelt noe er. Det er flere mulige risikofylte handlinger på sosiale medier, og noen av det vi legger ut der kan hjelpe en angriper med å utføre identitetstyveri. I og med at sosiale medier er et nytt medium, er det forskjell på hvordan folk bruker, og oppfatter risikoen. En kompromittert konto på sosiale medier gir en angriper tilliten til kontoeier ovenfor følgere/venner. I denne oppgaven viser jeg hvordan angripere vanligvis prøver å utnytte kontoer, å bruke dem til spam, phishing eller for å bruke lagrede kredittkort tilknyttet kontoen for å kjøpe annonser. Jeg viser også hva folk tror at kontoene deres kan brukes til av en angriper. Oppgaven viser at folk er veldig forskjellige i hvordan de oppfatter risiko, det er noen trender angående alder og kjønn, med den eldre generasjonen, som opplever høyere risiko og kvinner som oppfatter debatt deltakelse mer risikabelt enn menn. Resultatene mine viser at vi ikke har en enhetlig oppfatning av risiko på sosiale medier, og at offentlig diskusjon kan kvele grupper som oppfatter risiko som høyere enn andre. Disse resultatene viser også at en angriper vanligvis ønsker å utnytte tillit tilhørende kontoer, dette kan brukes til å påvirke opinionen.

Contents

Abstract	iii
Sammendrag	v
Contents	vii
Figures	xi
Tables	xiii
1 Introduction	1
1.1 Topic covered by the project	2
1.2 Keywords	2
1.3 Problem description	2
1.4 Justification, motivation and benefits	3
1.5 Research questions	3
1.6 Contributions	3
1.7 Thesis outline	3
2 Related work	5
2.1 State of the art for measuring risk perception	5
2.2 Previous works on identity theft and internet	7
2.3 Previous works on social media privacy, and risk	8
2.3.1 Previous work on compromised accounts	10
2.4 Summary	10
3 Method	13
3.1 Choice of method	13
3.2 Applied method	14
3.2.1 State of the art	14
3.2.2 Research questions 2, 3, 4 and 5	14
3.2.3 What are the consequences of identity theft in Norway	15
3.2.4 Data gathering	15
3.2.5 Data analysis	16
3.3 Summary	17
4 Results	19
4.1 Demographic and sample	19
4.1.1 Gender distribution	20
4.1.2 Age distribution	20
4.1.3 Municipality distribution	21
4.1.4 Education level	21

4.1.5	Social media used	22
4.1.6	Self-reported IT skill	23
4.1.7	How much people care about IT, information security and privacy	24
4.1.8	Update practices	25
4.1.9	Hacked profile	25
4.1.10	Password habits	27
4.2	Risk perception	27
4.2.1	Posting images	27
4.2.2	Posting about vacation	28
4.2.3	Posting about pets on social media	28
4.2.4	Posting or sharing news	30
4.2.5	Posting or sharing something political	30
4.2.6	Posting or sharing something humorous	30
4.2.7	Participating in a debate	32
4.2.8	Use snapmap	32
4.2.9	Posting/sharing and self-proclaimed privacy	34
4.2.10	Changed privacy settings	34
4.2.11	Visible information	35
4.2.12	Perception on what can be used in performing ID-theft	37
4.3	Compromised social media accounts	40
4.3.1	Reason for compromise	41
4.3.2	Consequences of social media ID theft	41
4.3.3	Activated measures	43
4.3.4	Would people click a possible phishing link	45
4.3.5	Insight form interviews	46
5	Discussion	47
5.1	Research question 1: What is the state-of-the-art approach for re- searching risk perception of ID theft?	47
5.2	Research question 2: What are the known consequences of social media ID theft in Norway	48
5.2.1	Value of information	48
5.3	Research question 3: How do people perceive the risk of ID theft on social media?	49
5.4	Research question 4: What data do people believe can be used by a possible attacker?	50
5.5	Research question 5: Does privacy concerns impact sharing habits?	50
6	Limitations and future work	53
6.1	limitations	53
6.1.1	Data gathering	53
6.1.2	Feedback from the questionnaire	54
6.2	Future work	54
7	Conclusion	57
	Bibliography	59

A	63
B Questionnaire	71

Figures

4.1	Comparison of gender distributions in %, for the different social media.	20
4.2	Comparison of Age distributions in %, for the different social media.	21
4.3	Comparison of municipality distributions in %, the population based on data from SSB vs. the questionnaire N=305	22
4.4	Comparison of education distributions in %, the Norwegian population based on data from SSB vs. the questionnaire N=305	22
4.5	Comparison of self-reported IT skill in %, for the different questionnaires N=329. 1 was very little skilled, and 4 was highly skilled in IT.	24
4.6	Shows in percentage how often respondents of the questionnaire update their devices N=313.	26
4.7	Comparison of hacked social media accounts distributions in %, for the different social medias.	26
4.8	Shows how people rate their perception of risk when they post images on social media.	28
4.9	Perceived risk when posting images of people being on vacation.	29
4.10	Shows how people rate their perception of risk when they post an image of their pets with names on social media.	29
4.11	Shows how people perceive risk when sharing news on social media.	30
4.12	Shows how people perceive risk when sharing something political on social media.	31
4.13	Shows how people perceive risk when posting/sharing humorous content on social media.	31
4.14	Shows how people perceive risk when participating in a debate on one a social media.	32
4.15	Shows how women and men perceive the risk of participating in debate on Facebook.	33
4.16	Shows how people perceive the risk of using Snapmap.	34
4.17	Asked to what degree they had limited the different kinds of information visibility, where 1 is that they have limited the visibility of the information minimally and 4 is that the visibility of the information has been limited greatly.	37

4.18 Comparison of how digital natives and non-natives rate to what degree their date of birth can be used in identity theft, represented in %, for the different age groups.	39
4.19 Comparison of how digital natives and non-natives rate to what degree their debit/credit card numbers can be used in an identity theft, represented in %, for the different age groups.	40
4.20 Comparison of how digital natives and non-natives rate to what degree their account and passwords can be used in an identity theft, represented in %, for the different age groups.	41
4.21 Example message that has been circulating from hacked Facebook accounts and sent to people on their friends list. https://nettvett.no/falske-videomeldinger-i-messenger/	45

Tables

4.1	Table showing answer rate with how many possible respondents there were on the platforms.	19
4.2	Comparison of the number of digital natives and non-digital natives.	21
4.3	The table shows the number of people who use the different kinds of social media. The first number is the number of respondents in that age group and the percentage is the percentage of people in the age group that use a given social media platform.	23
4.4	The table shows how often the respondents of the questionnaire post on social media. The total here is missing about 18 people, this was because of a issue that happened with the questionnaire. .	23
4.5	Comparison of self reported interest in IT in general, information security and privacy. The data is presented with the number of answers for each option and the percentage for the answer N=329. 1 was caring very little and 4 was care a lot.	25
4.6	Peoples answers on what their passwords habits are like N=329. . .	27
4.7	Anova of genders and people participating in debate on social medias, excluding the gender "prefer not to answer".	33
4.8	Shows descriptives of genders and participating in public debate on Facebook, excluding the gender "prefer not to answer".	33
4.9	Shows Person correlation between how much the respondents care about IT, information security, privacy and the perceived risk when performing different actions on Facebook.	35
4.10	Shows how people post on Facebook, in comparison to how much they said they cared about privacy, where 1 caring little and 4 is caring a lot about privacy.	36
4.11	Shows how many people have what kind of information visible and the percentage based on the number of total respondents on the questionnaire 329.	36
4.12	People were asked to rate to what degree they thought the different information could be used in performing ID-theft. The question asked was: To what degree to you think this information can be used against you to perform an identity theft against you? N=327-329(some people did not answer every question)	38

4.13	Anova between digital natives and non-digital natives seeing if there is a difference in how they perceive the risk with date of birth. . . .	39
4.14	Anova between digital natives and non-digital natives seeing if there is a difference in how they perceive the risk with debit/credit card numbers.	39
4.15	Anova between digital natives and non-digital natives seeing if there is a difference in how they rate account info and passwords. . . .	40
4.16	Shows the number of people who has had their account hacked. . .	41
4.17	Shows peoples answers on what they thought were their reasons of compromise N=47.	42
4.18	Shows categorised reasons for compromise from text answer in the questionnaire. The reasons have been grouped a bit together with other similar consequences N=47.	42
4.19	Grouped open answers for that a compromised account can be used for. N=329 with around 60 answers being blank or not relevant. . .	43
4.20	Measures users who have had their accounts compromised have activated to help mitigate a new compromise. N=47	44
4.21	Shows how often the people who had decided to use regular password changes as a control changes their passwords. N=13	44
4.22	Who the respondents thought they might get tricked into clicking a link if they received it from. N=314	45
A.1	Descriptives of the answers people gave about how they care about IT generally, information security and Privacy. where 1 is that they care very little and 4 that they care a lot.	63
A.2	Count of people how often people post on social media, looking at which people have gotten their accounts compromised	63
A.3	Shows how people post on social media, in comparison to how much they said they cared about information security, where 1 caring little and 4 is caring a lot about information security.	64
A.4	Shows Person correlation between how much the respondents care about IT, information security, privacy and the perceived risk when performing different actions on Reddit.	65
A.5	Shows how people post on Reddit, in comparison to how much they said they cared about privacy, where 1 caring little and 4 is caring a lot about privacy.	66
A.6	Shows how people post on Reddit, in comparison to how much they said they cared about Information security, where 1 caring little and 4 is caring a lot about information security.	67
A.7	Shows bivariate correlation analysiss of what people chose to answer between the platforms on the question about debating on a platform	67
A.8	Shows age and gender distribution for digital natives and non natives	67

A.9	Shows an Anova that uses gender as factor and the perception on the usability of different data in use for ID-theft.	68
A.10	Shows an Descriptives for gender and the perception on the usability of different data in use for ID-theft.	68
A.11	Shows descriptives for digital natives and non-natives to what degree they believe that information can be used in performing identity theft	69
A.12	Shows what demographic groups that have experienced having their accounts compromised.	69

Chapter 1

Introduction

Identity theft or hacked accounts are a big problem in today's interconnected society, one can look at the numbers of "compromised accounts" that *Have I been pwned* has in their database to see the magnitude ¹. Identity theft has never been easier than it is today, with most of peoples everyday dealings, including banking and their payments happening online. Furthermore, if we use the definitions mentioned later in the introduction, identity theft becomes an even bigger problem when we look at hacked/compromised accounts as a form of identity theft. In this thesis I want to explore how people perceive risk on social media, and how they believe that hacking on social media takes place, and how a hacked account is used.

There are a multitude of hacked social media accounts that have been misused to spread lies, phish and even used for stock manipulation. An example of a high profile social media account that was hacked could be Skype's Twitter account back in 2014. ² The hacked Twitter account was here used to post a tweet with the text "Don't use Microsoft emails..." Another example that most people might be more familiar with is a social media account that has been hacked and used to phish people or try to compromise more accounts. ³

Another use of compromised accounts that has been seen is with Facebook if one has a business account activated that lets people buy ads on their platform. Hackers who compromise the user's Facebook account can misuse the saved payment method to take out paid ads on Facebook⁴. These accounts can end up siphoning thousands of dollars from the victim's accounts before Facebook notices that something is fishy or the person who has had their account hacked manages to freeze or stop the payments.

With these incidents where an account has been compromised, it is interesting

¹Have I been pwned is a database consisting of leaked credentials for accounts, and with these leaked credentials the accounts can be looked at as compromised. <https://haveibeenpwned.com/PwnedWebsites>

²<https://www.theverge.com/2014/1/1/5264540/skype-twitter-facebook-blog-accounts-hacked>

³<https://nettrett.no/falske-videomeldinger-i-messenger/>

⁴<https://www.darkstardigital.co.uk/facebook-ads-account-got-hacked/>

to see how people perceive the risk they are exposed to when using social media. It is also interesting to see if there is any difference in how different age groups or genders perceive risk to be on social media platforms. There might be a difference in how people who are digital natives and non-digital natives perceive risks on social media (see definition later).

1.1 Topic covered by the project

The topic of this project is going to be to measure public risk perception of using social media, look at what people freely post and how this can be used by an attacker. The project consists of surveys sent out to users of social media to try measuring their risk perception when using social media. The survey was sent out through Slettmeg, Facebook, Twitter and Reddit.

1.2 Keywords

- Information security
- Social media
- Risk perception

1.3 Problem description

Social media is a very open platform where people tend to overshare. This oversharing might result in break-ins, a stolen identity, stalking and more, physical or virtual consequences. For example, houses being targeted while people are on vacation or accounts being stolen by an attacker using social engineering to trick the bankuser. Risk might not be the primary thing people think about when they post information online, even though they might be volunteering more information than one might think is prudent, had they shared the same information in real life/ in person.

I am going to use the definition for Identity theft from Datatilsynet(Norwegian data authority) and Norwegian punitive law §202

Norwegian data authority: 'Identity theft is when someone obtains, possesses, transfers, uses or appears as the rightful holder of an identification card or the personal information of a person to commit financial fraud, fraud or other crime.'

Norwegian punitive law §202:

With a fine or imprisonment of up to 2 years, the person who unjustifiably takes possession of another person's identity card, or acts with another's identity or with an identity that is easily confused with another's identity, with the intention to A. obtain an unjustified gain for himself or another, or B. inflict another loss or disadvantage

1.4 Justification, motivation and benefits

The Justification of why this study would be good to help society in awareness and to make people see the discrepancy on what information they choose to publish when they are on social media, and what information they give people face to face. It is also about giving everyday people some idea of what they post on social media can be used to steal their identity or perform other kinds of malicious acts against them. If people get a better idea of what information they are exposing, then their new awareness can help employers and other parties with interests that can be inhibited by malicious actors acting on the excess of information on social media.

1.5 Research questions

1. What is the state-of-the-art approach for researching risk perception of ID theft?
2. What are the known consequences of social media ID theft in Norway?
3. How do people perceive the risk of ID theft on social media?
4. What data do people believe can be used by a possible attacker?
5. Do privacy concerns impact sharing habits?

To solve these research questions, I did a literature review to find out what the state of the art approach in how I should measure risk perception. Furthermore, I measured risk perception out in the wild, and I measured how people use social media and what they share, and what consequences this can have.

1.6 Contributions

My contribution from this master thesis consists of information from victims of ID-theft/compromised accounts, what people have experienced as the fallout from having their social media accounts hacked. The thesis also contributes by highlighting what information people in Norwegian society have publicly available. The data used for the analysis was procured with a questionnaire where I had N=329 respondents. The questionnaire was designed to learn more about what compromised accounts on social media are being used for, what people have public on their profiles and how people perceive risk when doing different things on social media.

1.7 Thesis outline

This thesis consists of seven distinctly different parts that all try to build upon the previous parts:

1. **Introduction** this section consists of an introduction to the rest of the thesis. Furthermore, giving the reader a basic understanding of how the current situation is.
2. **Related work** the related work section consists of a literature review where previous works have been looked at for inspiration and answers on how the research questions can be answered.
3. **Choice of method** this chapter explains why I decided to do what I did when trying to explore the research questions, and it also explains the steps I took in performing analysis on results from the questionnaire.
4. **Results** presents the analysed data from the questionnaire.
5. **Discussion** this section discusses the research questions in regards to what was learned from the previous chapters. The discussion chapter also tries to come to some form of conclusion to the research questions.
6. **Limitations and future work** presents what could have been done differently or what other types of limitations this thesis has. The chapter also tries to come up with some new areas of interest based on what this thesis discovered.
7. **Conclusion** concludes the thesis and the research question.

Chapter 2

Related work

This section consists of previous work done on subjects relevant to answering some of the research questions, and how the other research questions can be answered. I have structured the related work section to tackle different subjects that are relevant for the thesis, looking at risk perception, Identity theft, Social media, and some works on compromised accounts.

2.1 State of the art for measuring risk perception

There are some different ways of performing a risk perception measurement. One way of doing it would be as Nina Gerber et al. [1] did with using risk scenarios and mental models to help participants of the study, in getting a grasp of what they are getting exposed to on social media. The study used three different risk cases to measure peoples risk perception, one about online social networks, one about smart homes, and the last one focused on smart health devices.

Rahim et al. [2] conducted a systematic review of approaches on how one can assess cybersecurity awareness. With this systematic review, they came up with some recommendations for what methods one should use when accessing risk perception. Most of the papers focused on organizations and their security awareness/perception, I used this paper and read through the ones about social media as the target demographic and where the home users where the demographic used. Most of the studies with these criteria used a questionnaire as their data collection methodology.

Furnell et al. [3] did another method for finding out peoples risk awareness. They surveyed 415 home users, and this study found its sample by email, word of mouth, and postings on forums that were frequently used by home users, this was done to ensure a broad comparable background. The survey targeted the UK demographic. 71% of the respondents of the survey were male. The survey creates different levels of knowledge that it puts participants into, these knowledge levels are self-reported.

The paper by Talib, Clarke and Furnell [4] tries to find out the level of awareness of people, and how their training from work has any effect on their security

awareness at home. This study was conducted over 49 days from August to October, with their target response number of 300. To measure the level of security awareness, the study used a 5 point scale where the participants rated themselves. This question was then tied into a question about competency with IT. An exciting part of this study is that it has some data on how people see personal information shared on social media.

In the paper by Kritzinger and von Solms [5] they give a theoretical model for E-Awareness, which is used to measure and train home users in the detriments of the internet. This model is supposed to be enforced by the Internet service provider (ISP) so that they can limit the scarier places of the web, and require people to take tests to see their awareness to go “further into cyber”.

Only one of the methods explored in the paper had their sample as people on social media Labuschagne et al. [6], and they wanted to create a game to increase the user’s security education through an exiting medium. In this game, they were going to use a quiz to determine the baseline of knowledge of the participants.

Marcon et al. wrote a paper about the risk perception in environmental surveys [7] here they use a scale for people to self-proclaimed their perceived risk. This scale consists of 4 different securities from “not at all” to 4 “a lot” they also included a “Don’t know” answer. They were given seven environmental issues and asked to rate the risk towards the health of a population, here the participants answered with the scale from 14.

Wu [8] does a literature review on how social media can pose a risk, his viewpoint is mostly based on that of a business with employees that use social media, but he does come up with some measures that laypeople without a business behind them can implement. One example of something a private citizen can do is to keep their software updated, implementing an antivirus and having a firewall turned on. He also points to some other papers that explore risk factors in social media.

Vargas [9] did a study where he tried to figure out the real value of personal information. One of the essential areas that he explored was the dark web and how much personal information, accounts and more get priced on this area. He found that personal information was indeed a commodity that was being traded on the dark web, and that it is something that should be looked at closer. For example, he found that different passports from different countries are being sold there. A passport from the UK which included a driving licence was listed at 51.99\$. Another passport from the UK with a utility bill and selfie was priced at 61.19\$.

Slovic, Fischhoff and Lichtenstein[10] had a study where they tried to explore and understand perceived risk more. In the paper, they explain that people when asked about the risk of something usually do not have any data readily at hand to help them calculate the risk, with the lack of data to use as a reference people usually end up using heuristics when assigning a risk value. These heuristics create a gap that experts should try to close when trying to discuss risk with a layperson.

Alhakami and Slovic [11] has a paper written about risk where he explores how risk and benefit relate to each other. They observed that if the perceived risk

were high, the perceived benefit would be perceived as low, and something that is perceived to have high benefit has perceived to have low risk. They had had questions they asked psychology students to rate the risk in regards to how risky something was towards the US. The students were able to rate the risks on a scale from 1- not at all risky to 7 - very risky. They found that in fact, perceived risk and perceived benefit correlate to each other.

In a paper by Slovic [12] he talks about the differences in how people perceive risk. The understanding of perceived risk between a layperson and an expert is different. He refers to studies he has done where they found that the public has a broader definition of what constitutes risk, where they include more dimensions to risk like Catastrophic potential, controllability and risk to future generations. Their opinion differs with the view from experts who has more of an impact and probability view on how they define risk. The international standards organization has in ISO27005 [13] defined information security risk as “potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization” with a note that it is measured by the combination of likelihood and consequence of an event.

Slovic et al. [14] talks in this paper about how past experiences changes how we perceive risk, and how heuristics changes how a person perceives the risk of an event. They mention how risks can be perceived by a person in two different ways which they have from Loewenstein et al. [15]; one is the rationale system which is about how people rationally react to risk, this would be the common understanding of risk consequence times likelihood. The other way he mentions we react to risk is the emotional reaction at the moment when an event happens. Loewenstein mentions that researchers should take into account the emotional reaction to risks.

Bickerstaff K. [16] has a paper about risk perception in regards to air pollution where she reviews different literature on the subject. As part of the literature review, she also goes quite in-depth on the subject of risk perception and how it has been handled in different literature. She also mentions, as Slovic does[14], that there is a gap between what experts and laypeople talk about as risk, and that what laypeople talk about as risk is multifaceted with differences between different communities, genders, nationalities etc.

2.2 Previous works on identity theft and internet

Hedayati [17] has written a conceptual review of identity theft. The paper brings forth the point that social engineering is usually used in performing an identity theft, where for example the attacker finds critical personal information about someone on their social media account and uses this information to gain trust from the victim's bank employees. From the information used in the paper, the author found that low tech identity theft was a lot more common than identity theft happening mostly online.

The paper from Lai, Li and Hsieh [18] explores the coping behaviour of people

towards identity theft. They designed their questionnaire on the literature review that they performed to ensure good quality. When possible, they used existing measures that were adopted. This paper investigated identity theft from the perspective of and doing an empirical study to show the effectiveness of coping approach, showing that coping helps in the prevention of identity theft.

Milne, Rohm and Bahl [19] looks at how consumers protect their personal information on the internet in regards to the threat of identity theft and seeing if there are any predictors for the level of online protection is practised. This study was done using three different surveys using multiple different demographics across the US. The surveys had some questions built upon the “best practices” for ensuring data privacy by the Center for Democracy and Technology (2003). This paper was inspiring to look at for how they researched identity theft.

Anderson [20] did a study to find out if different demographics had anything to do with the victimization of identity theft. This article was written using the data from the Federal Trade Commission’s survey from 2003. With the data from this study, Anderson found that older people have a reduced risk. The data for this study was from 2003, so there was not a lot of social media when created, and it seems like one of the biggest threats from the study was paying electronically for something, not something older people usually do. This article concludes that there seems to be a connection between demographic and the risk of being a victim to identity theft. The adoption of technology is probably higher now than what it was in 2003.

What happens to people after having been victims of identity theft is explored in the paper by Golladay and Holtfreter [21] where they explore the health detriments, as well as the emotional harms that being a victim of identity theft, can cause. They found that for example, age has an impact on the emotional response of a victim, where older people gets impacted more than younger people.

Jagatic et al. wrote a paper [22] where they tried to see if knowing the person who sends a phishing link impacts the trust in the link provided, this was done by emailing different students at Indiana University where they spoofed the sender of the emails, to create more trust towards the phishing link and site provided by an attacker. They found that people were much more likely to click and expose their information if the phishing link was provided this way. They created one control group and one where they spoofed the email, the control group had a 16 percent success rate, while the spoofed email one had a 72 percent success rate, showing that trust in the sender makes a big difference in a successful phish.

2.3 Previous works on social media privacy, and risk

Ur and Wang [23] constructed a framework for what a user of social media should ask themselves, to have the users from a diverse set of backgrounds have a good enough privacy according to their culture. One of the layers in the framework was a legal layer, and here, the Social media could ask themselves if they are compliant to for example European law, like the General Data Protection Regulation (GDPR).

The paper by Such and Cirado [24] explores not just the privacy implications of one person sharing information about him or herself, but includes people getting information disclosed about themselves from others posting information on social media platforms. The paper also shows several different coping strategies for how one can and should share information on social media, and what the main drawbacks these coping strategies might have. It also proposes some different strategies that can be used when posting multiparty privacy-related posts.

I had some trouble finding papers on social media and risk or social media and identity theft, so I broadened my search a bit and included Open-source intelligence (OSINT) into the social media searches since this will be an accurate representation on what an attacker can get from social media in regards to data.

Ivan, Lov, Lutai and Grad [25] wrote about open source intelligence methods that can be used on social media. The paper mentions that using OSINT on a social network can be quite time consuming since there is so much information there for an analyst to go through. The paper does reference that the most potent legitimate reason for an analyst to go through data on a social media platform is to ensure national security interests, this is part of the “I’ve got nothing to hide” argument that Solove [26] had a little disagreement. This paper was primarily focused on the usability of data from social media as a data collection method for analysts, referring to the practice as Social media intelligence (SOCMINT). SOCMINT is a method for social media intelligence gathering written about by Omand, Bartlett and Miller [27] where they set some guidelines that they feel should be followed by a country when performing open-source intelligence gathering on a social platform.

Baccarella, Wagner, Kietzmann and McCarthy [28] wrote a paper about the dark sides of social media. They used a honeycombed pattern to illustrate the different ways of how social media can be detrimental. They mentioned sharing and online identity, among others, as two of these seven building blocks that create the dark side of social media. They mainly focused on online harassment and other types of psychological strain that might be associated with active social media use. The only mainly physical concern that the paper mentioned that could come from social media was stalking, where one tends to share geographic location during messaging or posting.

D.Irani et al. [29] talk about how a person can be tricked into pursuing some kind of a relationship with an attacker. For example, they explore how the recommended friends section on Facebook can be played to have an attacker higher up on the list to get a potential victim to initiate the contact, and be more invested in the relationship between the two parties. This approach of sneaking into the recommendation list was one of three different approaches that D.Irani et al. explored; the other two were: Demographic-based, often seen in dating sites where the site tries to match people with the same characteristics. The last one they explored was visited based; this can be found in, for example, LinkedIn where the site lets a user see who has been visiting their profile. They found that a female profile is about 2 - 40 times higher than a worse performing profile. They also

found that the pretext of an approach was also very important like it was expected to be. These kinds of reverse engineering attacks where the user initiates the communication could also be more focused on targets, by tailoring the profiles more towards specific people.

Egele, Stringhini, Kruegel and Vigna wrote a paper about detecting compromise in social media [30], they used messages that were sent from social media accounts to create profiles on users, and this normal usage behaviour was used to monitor for suspicious activity. They focused mostly on what kind of damage a hacked high profile account can do if it is not stopped or noticed early, they exemplify with news outlets getting hacked and tweeting about the death of Obama, and Skype getting compromised and messages staying up for hours.

Warner-Sønderholm et al. [31] have a paper exploring the trust in social media, and the trust people have in social media as a news source. They found that women and people younger than 20 seemingly had a higher level of trust in social media. The level of trust also rose, the more people were using social media. They also checked if the level of trust impacted how much people trust newsfeeds on social media. They ended up finding that the three groups mentioned whom they found had higher trust towards social media, also had a higher trust in the social media newsfeed.

2.3.1 Previous work on compromised accounts

Thomas et al. [32] had a year-long study where they explored exposed credentials and the match rate with google accounts. They had three datasets they used for the leaked credentials during the study, one from just usual credential leaks, one from phishing kits and the last one from keyloggers. They found that from the credential leaks they looked at, there was a match rate of 6.9 %, The phishing kits had a match rate of 24.8 % and the keyloggers match rate was 11.9 %. The match rate they talked about was still active and usable credentials.

Nyblom, Wangen, Kianpour and Østby [33] used a root cause methodology to find out what the root cause of compromised accounts were at a university. They found that one of the most significant contributors to compromised user accounts had been the reuse of credentials on different sites which made up 42% of the hacked accounts, the next was password strength at 25%, malware at 19 % and phishing at 10%.

2.4 Summary

There has been a lot of different works done on risk, risk perception and risk awareness. Risk is usually defined as the consequence and probability of something happening, but this definition might be a little bit too narrow for when measuring risk in laypeople. Because as Slovic mentioned [12], the heuristics of a person has an impact in how they perceive and rate risk. Bickerstaff K.[16] mentioned that most risk perception studies at the time had been conducted mostly

in with questionnaires, but that more recently more studies had started to use, or supplement their quantitative data with qualitative data as well. There does not seem to be many papers written about the risk perception of people when it comes to social media and especially how people perceive the risk of a compromised social media account. I want to try to fill this gap in the literature with my thesis. By asking people about how they perceive the risk, what they think a compromised social media account can be used for, and the experiences of people who have had their accounts compromised.

Chapter 3

Method

The method chapter is set up to make it easy to find out what and how the survey and research have been conducted, for those who might want to do a similar study. In this chapter I will firstly discuss the possible research strategies available for my masters project. The topic for the latter part of the chapter is about choices made and why. The method chapter is set up so that others who might want to do a similar study, or there are faults in the thesis can easily find out what has been done. I will also include a summary of the applied method at the end.

3.1 Choice of method

There are many different ways one can go about researching risk perception and risk awareness of people. As seen in the related work section, one approach was to measure the risk perception of people. One of the most usual approaches would be like Alhakami and Slovic [11] did in their paper and performed a questionnaire towards students. They had some questions that they split into two groups so that the questionnaire would not take too long to perform. Another way I could have done my data gathering could have been physical interviews, getting more qualitative data, this was not done because of the time required to find people that are diverse enough to get an excellent demographic sample for the study, and the difficulty of reaching out to different people in half a year. With that said I would have liked to have been able to do some questions more in a proper case study where I could have looked more at someone's actual response, do a proper test and see what and how people react to a phishing message on Facebook, do people click the link or do they not, and what gives a higher hit rate. Such a case/phishing test would probably if performed on friends/family be unethical to perform, like phishing tests are always criticized, Like Jørgen and Roar from NSM discussed in the NSM podcast ¹. Such a phishing test could have helped explore how people perceive the risk with received messages on social media, and how familial or relationships change how people perceive that risk. The best way for this thesis

¹<https://www.nsm.stat.no/blogg/podcast---phishingkampanjer---trenger-vi-a-teste-ansatte/>

is with these things in mind doing a questionnaire, where I could reach out to a bigger audience and get better representation on the survey, it is also quicker to perform than doing a lot of more significant interviews with different people. This questionnaire could also be supplemented with some short interviews where I ask people who show interest for interviews and have had their accounts hacked, about their experiences trying to supplement the data on the known consequences of identity theft.

3.2 Applied method

Here I will talk about the actual method that was applied in the thesis, and the section is structured after the different research questions for how data on the different topics are gathered and a later section that explains how data was analyzed for the study.

3.2.1 State of the art

To find out what is state of the art for researching risk perception and identity theft, I looked at previous works done in risk perception and identity theft. The information gathering for what is considered state of the art was done in the related work section. From there, the rest of the master thesis built on what was found in these works. I tried to use what was found in related works when measuring people's risk perception with a questionnaire.

3.2.2 Research questions 2, 3, 4 and 5

These research questions were explored by conducting a questionnaire to gain information about the topic and to gain data for this thesis. This questionnaire was a quantitative one, so I tried to get as many people as possible. I also performed some qualitative interviews with a couple of the respondents of the questionnaire, the people I could contact again who had had their accounts compromised had to come from the Slettmeg questionnaire where I asked for email addresses.

When creating the questionnaire, I tried doing like Milne, Rohm, and Bahl [19] and create some questions using the current best practice advice from a trusted authority on how not to get one's identity stolen. Using Norsis advice and guidelines on how to prevent identity theft ² to find out if the survey respondents are following best practice. I made some questions where I tried to gauge more on what people have posted and readily available on their profile, for example, email or phone number, which both can make it easier to break into someone's account if an attacker has access. I also had some questions about the risk of posting in general, whether it was posting pictures showing that you are on vacation, which could increase the risk of having your home broken into. To answer

²<https://nettvett.no/forebygge-identitetsverdi/>

research question 5, I asked the respondents of the questionnaire if they had experienced having their social media profile compromised, and if they had, I asked them about the consequences of this compromise. In the Slettmeg questionnaire, I also asked people for their email address so that I could be able to reach out to people who had experienced compromise, and hear if they had any more information about the experience, but from the limited pool of compromised accounts, only two people answered some further questions.

3.2.3 What are the consequences of identity theft in Norway

To get a proper answer to the second research question, I asked people who have been exposed to identity theft about their experiences about the ordeal. I had two qualitative interviews to get a deeper understanding of the impacts of successful identity theft in Norway. However, it is not necessarily easy for people to figure out what an account was used for; some times, it seems like an account takeover has next to zero actual consequences. From working at Slettmeg, I have seen some Facebook accounts just be taken over and have the name and picture of the account changed, this as an example. Would a person who has their account taken over in this fashion reflect over why this was done, or write that there were no consequences. For them, the consequence was that they lost access to the account for a while, but maybe not how the account ended up being used. Furthermore, why does a hacker change the information of an account? Is it done to increase the lifetime of an account used for phishing schemes, or is it for the *street cred* one can get in a hacking community?

3.2.4 Data gathering

The sampling was done with three different questionnaires distributed on three “platforms”. I had one questionnaire that was distributed through Slettmeg.no. One was distributed generally through Facebook and Twitter. This version was mainly distributed through my social media network and on the Facebook group “Kode 24- gruppe”. The last one was distributed through Reddit.

The Slettmeg questionnaire was the questionnaire that was distributed first, and some changes got implemented between this questionnaire and the two that were distributed through social media. In the Slettmeg version the main question asked was formulated as “How aware are you to risk when you perform the following on (social media)” this was changed into: “How do you perceive risk when you perform the following actions on (social media)”, this was done to ensure that what is measured was risk perception, and not risk awareness.

Sampling

The sampling ended up being a bit all over the place; this happened because I started just wanting to survey Slettmeg to get answers from many people having experienced compromised accounts. I wanted to have as many people who had

experienced having their accounts compromised as I could, and for this objective, Slettmeg seemed like an excellent arena for distribution. The response rate from Slettmeg ended up being a bit lacking in the number of people we reached out to being low, so to increase the number of respondents to my questionnaire and get a better data set. I ended up doing a convenience sampling and sending out the questionnaire as widely as I could through Facebook/Twitter and supplemented that with Reddit to get a broader demographic data set, not concentrated around my circle of friends, that Facebook ended up giving me. Facebook and Reddit being added caused some imbalances in the demographic data of the study, were Reddit had a tiny amount of women that use r/Norge, which was the Reddit group used to send out the questionnaire. Gelinis et al.[34] wrote a paper about ethical considerations when using social media as a recruitment platform, they created a checklist of things that one should consider before using social media for recruitment. To try to be as transparent and above board as possible when distributing the questionnaire, I asked for permission from one of the administrators on the "Kode 24" Facebook group before posting there, and the post where I asked for participants made it very clear that participation was voluntary and sharing would be greatly appreciated.

3.2.5 Data analysis

For the analysis part of the master thesis, I started mapping out the demographics of the respondents. The demographic data was sorted by where the data stemmed from; this was done to show the differences between the social media platforms and to get a better understanding of how these groups differ demographically. The analysis started with me doing some descriptive analysis univariate analysis to create some histograms and look more closely at the collected data. I did this for all the different answers that I got in the questionnaire to be able to look more closely at how people answered the questions.

After the demographic data was established, the analysis of the rest of the data was performed, looking at/for trends in the data set and presenting the answers in either tables or figures in the results section.

The data analysis in this thesis is mainly done statistically to analyze the data from the questionnaire. I used Anova analysis to see if there are any differences between the groups in the dataset. Checking to see if gender or age have any impact on how people in Norway perceive risk on social media, and if either of these variables change the sharing habits or their exposure to having their accounts compromised. We can also split the collected ages into digital natives and non-digital natives; there might be a difference in how the digital natives perceive risk on social media. Gkioulos et al. [35] defined digital natives as people born between 1987 and 1997. I chose the age group <31 as digital natives and those at the age and over 31 as non-natives, this was done to have my numbers as close to theirs as possible.

The use of ANOVA or other bivariate methods for analyzing ordinal nonlinear

data has been criticized for not being normally distributed, like the data in this analysis is going to be. Norman[36] wrote a paper about different aspects of tension for when one can use ANOVA or other bivariate analysis, and used earlier studies to back up that there is little to no reason not to use bivariate analysis on nominal data such as Likert scales, small sample sizes or data that do not follow a normal distribution.

3.3 Summary

To give a quick summary of how what method I used during this thesis. I started with creating a questionnaire and did some quality control with some friends and family, fixed issues. The questionnaire was sent out to people who agreed to receive the questionnaire on Slettmeg. When I noticed after a couple of weeks on Slettmeg, that I did not receive as many answers as I had hoped for. I did some revisions on the questionnaire before I distributed the questionnaire (in Appendix B) out on Facebook/Twitter and Reddit. The distribution on Facebook/Twitter was done mostly by posting it on my profile, but I also made a post on a Norwegian coding community. The Reddit one was distributed on the Norwegian subreddit r/norge.

When it comes to the Data analysis, this was done with first analyzing every variable separately, looking at trends and distribution with histograms and descriptives. When this had been done, I performed some Bivariate analysis, ANOVA on age and gender to see if age and gender had any effect on the answers given and to test for significance between groups. I also performed a Pearson correlation with the data on how much people care about IT, information security, and privacy to see if this had any effect on how people perceive risk.

Chapter 4

Results

This chapter takes the answers from the distributed questionnaires and analyses the answers from the questionnaire. The chapter consists of three different sections, demographic sections that explore what the sample consists of, a risk perception section about the answers on how the respondents perceive risk on social media. The last part is about the answers given about compromised accounts.

4.1 Demographic and sample

This section takes the demographic answers from the questionnaire and presents them. Not all the demographic questions were asked in the Slettmeg distributed questionnaire; this was done to avoid databases being comparable and ensuring the anonymity of the respondents. The number of answers from the different questionnaire are as followed: Slettmeg N=24 ,Facebook/Twitter N=198 and Reddit N=107. Table 4.1 shows the number of people who could have answered the questionnaire and the number of people who answered it. For Slettmeg it shows number of possible as the people who received an email asking if they wanted to participate. Users from Facebook is estimated from friends of the people who shared my post and an average of the friends multiplied by the number of people who had hidden their friends list, and the Reddit number is from people subscribed to r/norge. There is no way to check the number of people who saw the post on r/norge but the post received nine likes at the with a 72% upvote rate.

	Number of possible users	Achieved	Percent
Facebook/Twitter	7 286	198	2,7%
Reddit	133 000	107	0.08%
Slettmeg	123	107	20%

Table 4.1: Table showing answer rate with how many possible respondents there were on the platforms.

4.1.1 Gender distribution

The gender distribution varies greatly between the different platforms the questionnaire was distributed. We can see, for example, that Reddit has a very skewed gender distribution, with most of the people on the platform being male. The distribution can be seen in figure 4.1. The gender distribution can also be compared to that of the Norwegian population as a whole, taken from Statistics Norway (SSB)¹ we get to have 50.19 % males in the age 18 years or older and 49.81% females 18 years or older, as of 2020. So we can see that from the data set the convenience sampling skewed the genders towards being primarily male. The data set from SSB only includes the genders male and female and do not take other considerations when presenting the data.

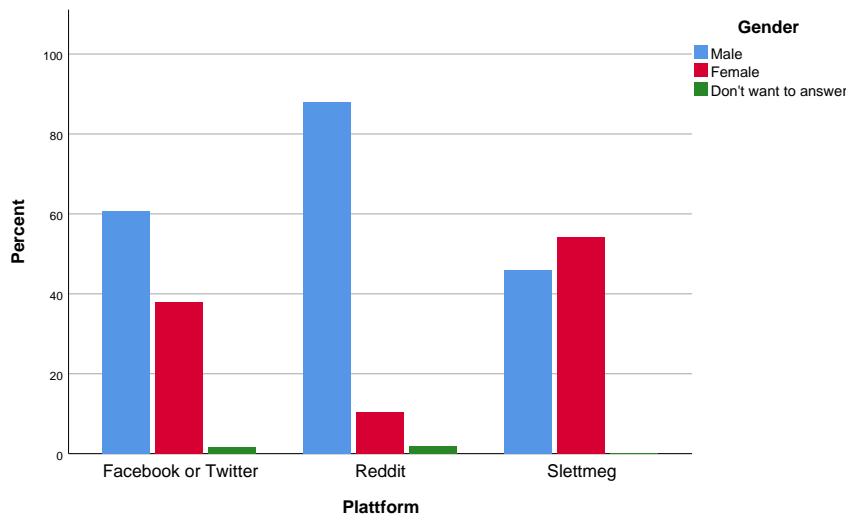


Figure 4.1: Comparison of gender distributions in %, for the different social media.

4.1.2 Age distribution

The age distribution from the respondents can be seen in figure 4.2. The age distribution is highly skewed towards the younger generations, that is most likely an effect of the distribution on Facebook and Twitter happened with me posting it on my social media profile, and many people from my age group answering. To help mitigate how skewed the data is, we can split the age groups into two big groups, digital natives people at the age of 30 or younger, and non-digital natives people older than 31, see table 4.2. To get as close to the definition of digital natives proposed by Gkioulos et al. [35], the split between the two age groups ended up being 30 and 31.

¹<https://www.ssb.no/statbank/sq/10036277>

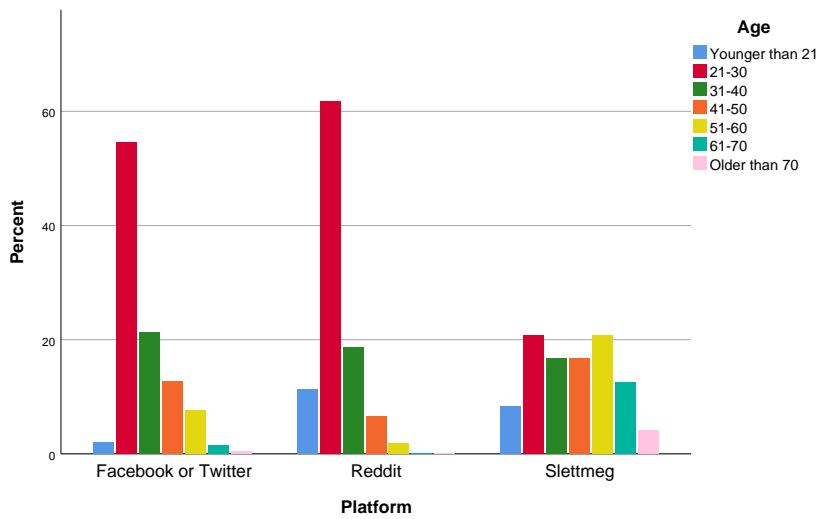


Figure 4.2: Comparison of Age distributions in %, for the different social media.

	Count	Percentage
Digital natives (younger than 30)	197	59,90%
Non-digital natives (31 plus)	132	40,10%

Table 4.2: Comparison of the number of digital natives and non-digital natives.

4.1.3 Municipality distribution

The municipality distribution in figure 4.3 shows the difference between the population in Norway, this data has been taken from SSB. The difference between the population can mostly be seen with Oslo and Innlandet; this is probably because of the convenience sampling through Facebook and me having studied in Oslo and Innlandet ². The discrepancy in municipalities compared to that of Norway in large probably will not impact the later answers because how people use social media is probably the same across the country.

4.1.4 Education level

The figure 4.4 shows the educational level of the respondents of the questionnaire; the Slettmeg questionnaire is not a part of these statistics because the educational level was not asked there. Compared to the education level in the rest of the population, the respondents of the questionnaire have, in general, a higher level of education. This difference might stem from a sampling bias caused by most of the sampling happening through my network on social media and me getting help with sharing the questionnaire from other people I have met at university.

²<https://www.ssb.no/statbank/sq/10036698>

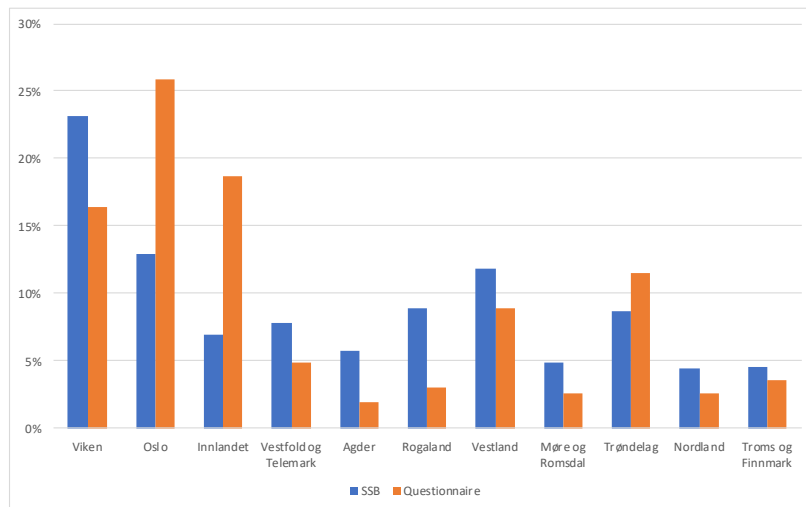


Figure 4.3: Comparison of municipality distributions in %, the population based on data from SSB vs. the questionnaire N=305

It might skew the risk perception a bit if a lot of the people who answered the questionnaire are from the same educational background as me, and have a more straight forward understanding of risk, with risk solely being consequence times probability of an event happening, like Slovic[12] mentioned there are differences in how laypeople and experts define risk.

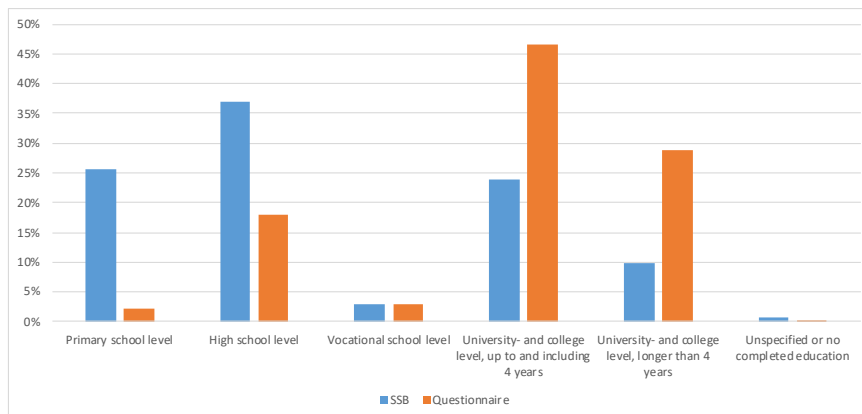


Figure 4.4: Comparison of education distributions in %, the Norwegian population based on data from SSB vs. the questionnaire N=305

4.1.5 Social media used

The people who participated in the questionnaire used the social media shown in table 4.3. Since every person may use multiple social media platforms, the total amount exceeds the number of respondents of the questionnaire. From the table,

we can see that there are at all ages, more than 65% of people using Facebook as a social media platform. The numbers for Facebook keep climbing the older people get; this is interesting, with most of the other social media having a reverse distribution from Facebook, at least down to around 21-30 demographic, which peaks in all the other named social media platforms. The age group that has the highest percentage of people using another social media platform than the ones named is 41-50 group.

Age	Facebook		Instagram		Twitter		Reddit		TikTok		Snapchat		Other		N
Younger than 21	12	66.7 %	12	66.7 %	11	61.1 %	14	77.8 %	6	33.3 %	14	77.8 %	3	16.7 %	18
21-30	156	87.2 %	116	64.8 %	73	40.8 %	121	67.6 %	18	10.1 %	158	88.3 %	22	12.3 %	179
31-40	59	89.4 %	38	57.6 %	25	37.9 %	41	62.1 %	3	4.5 %	53	80.3 %	7	10.6 %	66
41-50	33	91.7 %	26	72.2 %	16	44.4 %	11	30.6 %	3	8.3 %	27	75.0 %	8	22.2 %	36
51-60	20	90.9 %	13	59.1 %	8	36.4 %	2	9.1 %	2	9.1 %	12	54.5 %	2	9.1 %	22
61-70	6	100.0 %	4	66.7 %	1	16.7 %	0	0.0 %	0	0.0 %	2	33.3 %	1	16.7 %	6
Older than 70	2	100.0 %	0	0.0 %	0	0.0 %	0	0.0 %	0	0.0 %	1	50.0 %	0	0.0 %	2
Total	288		209		134		189		32		267		43		329

Table 4.3: The table shows the number of people who use the different kinds of social media. The first number is the number of respondents in that age group and the percentage is the percentage of people in the age group that use a given social media platform.

The respondents of the questionnaire were also asked about how often they post on social media, table 4.4. From the table, we can see that 53 % of people post on social media more rarely than once a month. 22 % post at least once every month on social media, 14% post around 0-5 times in a week, this shows that most people use social media kind of passively, with posting 89% posting less than once a week.

	Count	Percentage
More seldom	165	53%
1-3 times a month	69	22%
0-5 times a week	43	14%
6- 10 times a week	18	6%
11-15 times a week	1	0%
16-20 times a week	3	1%
More often than 20 times	12	4%
Total	311	

Table 4.4: The table shows how often the respondents of the questionnaire post on social media. The total here is missing about 18 people, this was because of a issue that happened with the questionnaire.

4.1.6 Self-reported IT skill

The figure 4.5 shows how the respondents rate their skills concerning IT. As we can see, very few people rate themselves as “bad” with IT with the lack people choosing 1, it might also be that most people who would have chosen 1 in their

IT skill dislike IT so much that they opt out of using social media platforms, such as Facebook or Reddit. From the figure 4.5 we can see that from both the questionnaire distributed on Reddit and Facebook/Twitter that around 15 % of the respondents chose that their IT skill level was at 2, this is in stark contrast with the questionnaire distributed on Slettmeg, where approximately 55% of people chose the same. For all three, around 40% chose that their IT skill was at a 3, And about the same amount of people placed their skill level at 4, from the Reddit and Facebook/Twitter questionnaire, zero people placed themselves at highly skilled in the Slettmeg distributed questionnaire. That Slettmeg has such different values here could come from who decides/needs to use their service.³

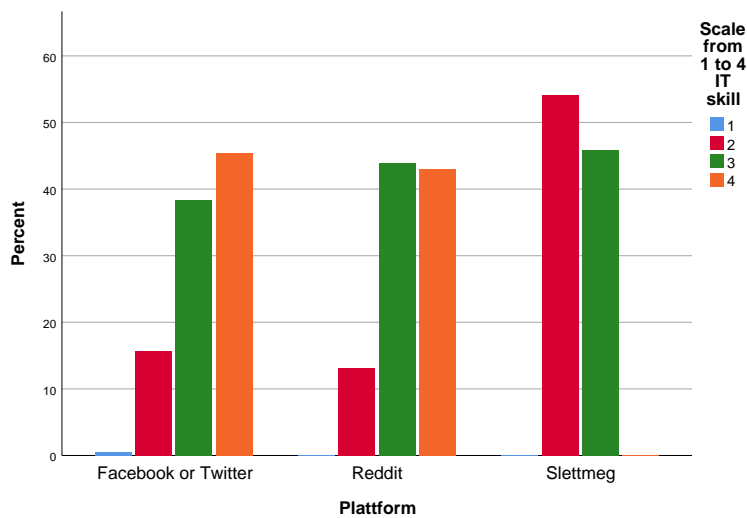


Figure 4.5: Comparison of self-reported IT skill in %, for the different questionnaires N=329. 1 was very little skilled, and 4 was highly skilled in IT.

4.1.7 How much people care about IT, information security and privacy

In the table 4.5 we can see how much people care about IT, information security and privacy. From the table 4.5, we can see that for IT generally has a lower number of people caring about it. Information security and privacy are pretty similar in peoples enthusiasm towards the subject, but people seem to generally care a little bit more about privacy, the descriptives can be found in the appendix table A.1.

³Slettmeg is a service that helps people who feel offended online, and the work with knowing where to contact sites, etc. to help people remove the offending content. <https://slettmeg.no/om-oss/>

	Choice	Count	Percentage
IT generally	1 Caring very little	9	2,70%
	2	78	23,70%
	3	107	32,50%
	4 Care a lot	135	41,00%
Information security	1 Caring very little	6	1,80%
	2	39	11,90%
	3	148	45,00%
	4 Care a lot	136	41,30%
Privacy	1 Caring very little	4	1,20%
	2	44	13,40%
	3	133	40,40%
	4 Care a lot	148	45,00%

Table 4.5: Comparison of self reported interest in IT in general, information security and privacy. The data is presented with the number of answers for each option and the percentage for the answer N=329. 1 was caring very little and 4 was care a lot.

4.1.8 Update practices

The respondents were asked about how often they update their system, and the update routines can be seen in figure 4.6. From the figure, we can see that there are not that many people who participated in the questionnaire that own a tablet device, less than 52%, 93% of the respondents own a PC/Mac and 99% of the respondents have phones. We can see that most people update their devices as soon as they receive a notification about updating. There are about 6 % of people that keep withholding updating their systems. The recommended frequency of how often one should update their devices is as soon as a patch is available, or as soon as possible, according to Roar Thon in Norwegian National Security Authority (NSM)⁴. Windows has a monthly security patch that goes out on a Tuesday also known as, patch Tuesday, so for pc/mac about 88% of people are probably up to date or at most one month behind.

4.1.9 Hacked profile

In figure 4.7, one can see the percentage of people who have had their social media account hacked. As one can see, the percentage of hacked accounts is quite a bit larger from the Slettmeg questionnaire; the reason for this is because Slettmeg also helps people with regaining access to their hacked accounts. The Facebook and Twitter(N=198) questionnaire has about 13% of the respondents had experienced having their account compromised, with Reddit(N=107) about

⁴<https://www.dn.no/teknologi/teknologi/datasikkerhet/microsoft/innlegg-sla-pa-automatiske-oppdateringer-unnga-datainnbrudd/2-1-654083>

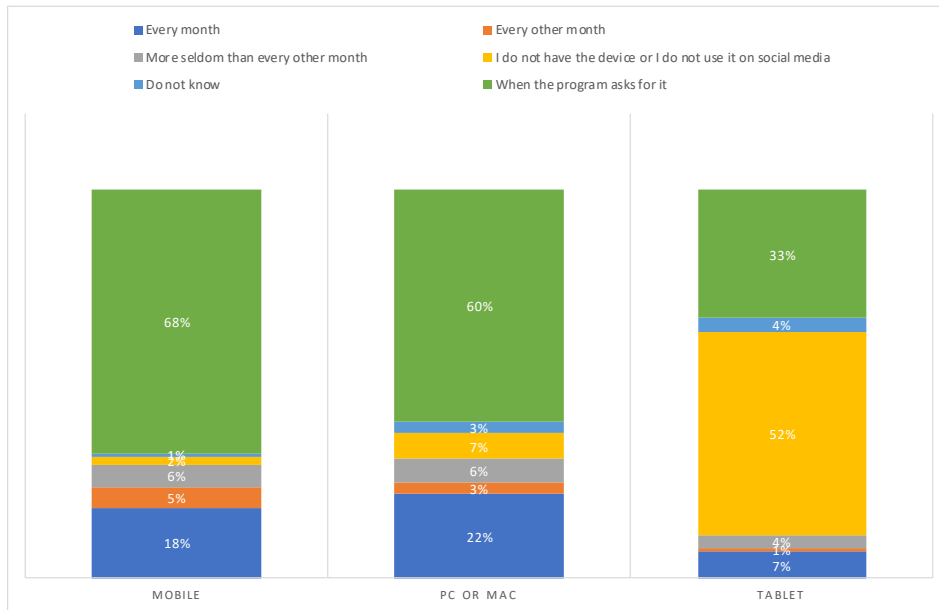


Figure 4.6: Shows in percentage how often respondents of the questionnaire update their devices N=313.

11% of people in the questionnaire distributed there had experienced a compromised account. Lastly, from the questionnaire distributed to people contacting Slettmeg (N=24), about 42% of people had experienced a compromised account. So, if we are talking about the population as a whole, the percentages from Reddit and Facebook/Twitter are probably more representative than that of Slettmeg, with Slettmeg helping people who have compromised their accounts.

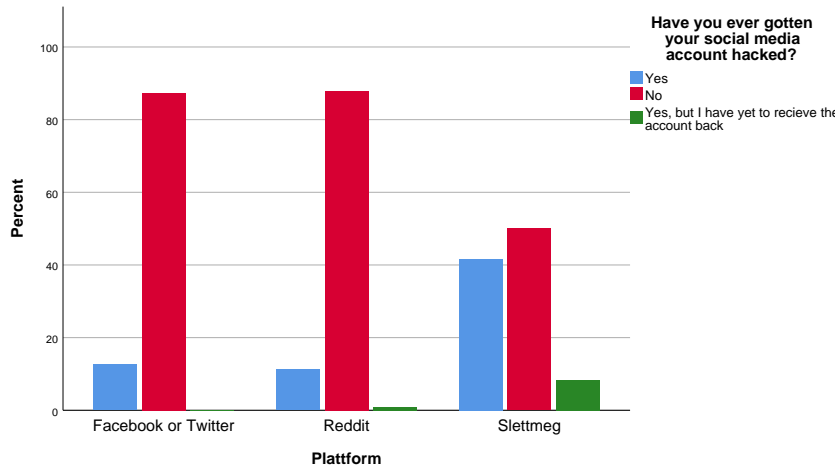


Figure 4.7: Comparison of hacked social media accounts distributions in %, for the different social medias.

4.1.10 Password habits

Passwords are what most websites use to authenticate a person and give them access to their account on the site. Back in 2017, Thomas et al. [32] found that just from data leaks, 7.5 % of credentials were still active and usable. We can see from the answers from the questionnaire in table 4.6 that our respondents too are probably around this number with 3 % using the same password everywhere and 9.4 using the same everywhere but 2-factor authentication if it is available. For people who use close to the same password, there were 28.6% of people. They had the same password but used small variations on it for different sites, to keep the passwords unique.

Do you use the same password on social media as on other sites?	Count	Percentage
I always use the same password for everything	10	3.00%
I use the same password for everything but 2fa where possible	31	9.40%
I use small variations of a password on differing sites	94	28.60%
I always use different passwords	55	16.70%
I use different passwords and 2fa where possible	139	42.20%

Table 4.6: Peoples answers on what their passwords habits are like N=329.

4.2 Risk perception

One of the questionnaire's main questions was asking people how they perceive the risk of doing certain activities when utilizing social media. The questionnaire did not ask all the same questions about all the different social media platforms; this was done not to tire out the respondents of the questionnaire. For example, I did not include the risk perception questions about Reddit on the questionnaire distributed on Facebook/Twitter, but I felt that it was needed on the questionnaire distributed on Reddit. For the questions regarding the risk perception on social media, the N values for the platforms were as following: Facebook N=265, Twitter N=131, Reddit N=107, Snapchat N=249.

4.2.1 Posting images

The figure 4.8 shows that very few think posting images is a high-risk endeavor. Reddit users are the ones who rate their perception of posting images as the riskiest with 14 % of the user saying high and 7 % saying very high. Both Reddit and Snapchat have about 20 % more respondents perceiving the risk of posting images as very low. Images can contain quite a bit of metadata that can be used to figure out quite a bit about the camera used when checked, some cameras even include the geotagging of where the picture was taken[37]. All this information could be used for stalking purposes, and one could figure out if the device that has taken a photo is vulnerable to some exploit, if the model and make is vulnerable.

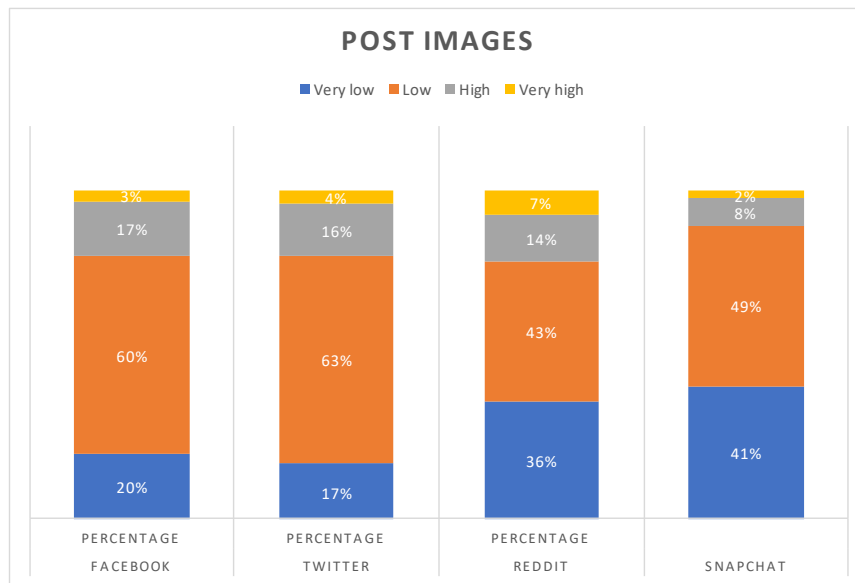


Figure 4.8: Shows how people rate their perception of risk when they post images on social media.

4.2.2 Posting about vacation

This question was asked to gauge how people perceive the risks that can come from posting about a vacation on social media, an example that has been seen is people having their houses broken into while on vacation, while it is uncertain that thieves use OSINT to find victims or not, the threat is there and easily visible. Figure 4.9 shows how people perceive the risk of posting about their vacation. The question asked the respondents how they perceive the risk of posting that they are on vacation. As we can see from the figure, the perceived risk goes higher with the highest perceived risk from Twitter users, where they placed about 60 % as high or very high. Reddit and Snapchat seem to have a lower perceived risk than Facebook and Twitter; this might stem from the more direct form of interaction with Snapchat and the more anonymous interaction with on Reddit.

4.2.3 Posting about pets on social media

This question was asked to gauge a bit of how people perceive the risk in posting about something that very likely could show up as a security question on one of the services that they use. We can see how people answered this in figure 4.10 Here, the people only we had at most 27 % that perceived the risk to be high or very high. The interesting part about this question is that it could be a security question that someone in a household uses. Even though the risk of compromise is not huge for you, because it is the second dog, it might be someone else's first, and then be used in a security question. I believe security questions like this one is in the process of being phased out because of how easy it is to gain information

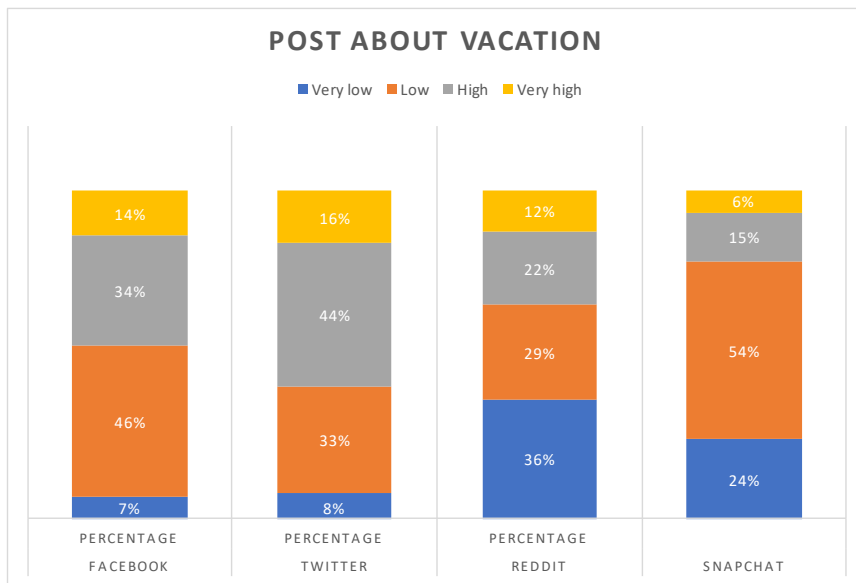


Figure 4.9: Perceived risk when posting images of people being on vacation.

on social media, but it is interesting to see that there are very few people who perceive risk in posting pet images.

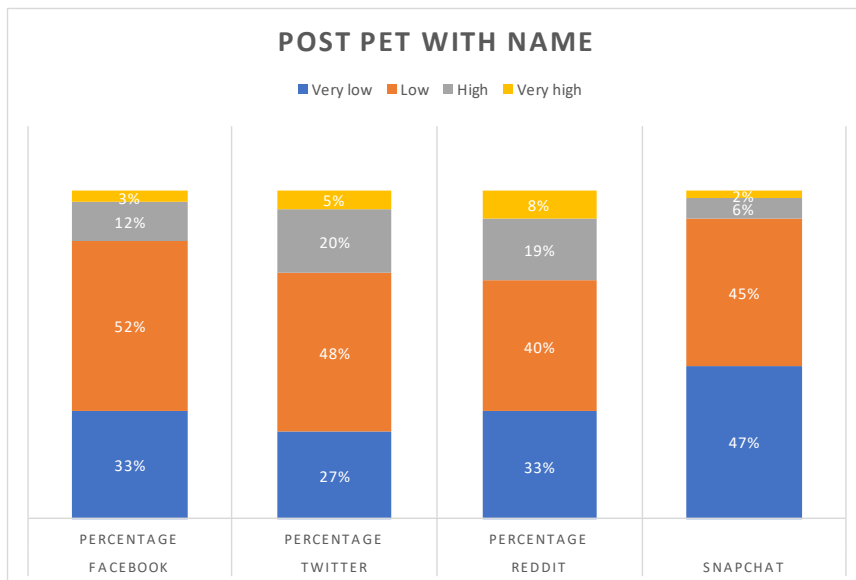


Figure 4.10: Shows how people rate their perception of risk when they post an image of their pets with names on social media.

4.2.4 Posting or sharing news

Figure 4.11 shows how people perceive risk when sharing or posting news-stories on social media. Here high and very high comes to about 18 % at the most; this shows that very few people perceive the risk of sharing or posting news as generally low. around 55% rate the risk as low on Twitter and Facebook, Reddit has it at 39%, and around 27% on Facebook and Twitter rate it as very low risk, 53% for Reddit.

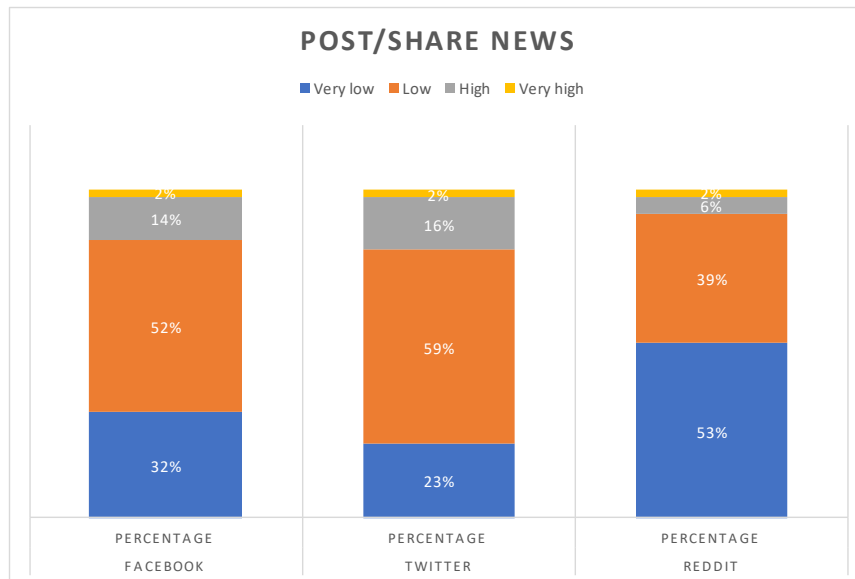


Figure 4.11: Shows how people perceive risk when sharing news on social media.

4.2.5 Posting or sharing something political

The question about people posting or sharing something political was asked to gauge if people find that exposing their political beliefs on social media can be risky/damaging. In figure 4.12, we can see that the users of Twitter have the highest perception of risk with 37% on high and 11% on very high. Reddit is again quite far behind the other two social media with it is 22 % on high or very high, this might again be because of the more anonymous nature of the Reddit as a social media.

4.2.6 Posting or sharing something humorous

The perceived risk of posting or sharing something humerus can be seen in figure 4.13. Twitter perceive the risk to be highest with 11 % at high and 2 % at very high. Both Snapchat and Reddit have their very low perceived risk at around 50 %. Humor has shown that it is a good way to spread propaganda, we saw many

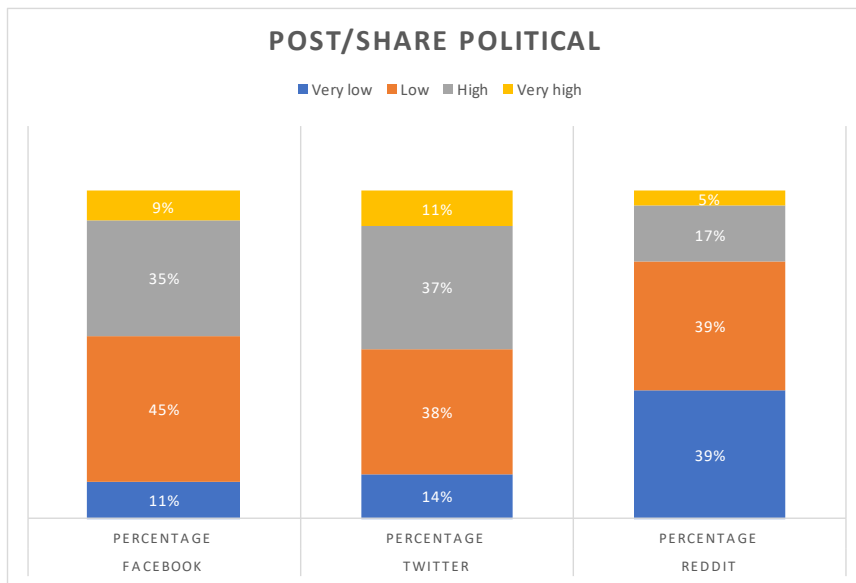


Figure 4.12: Shows how people perceive risk when sharing something political on social media.

memes get weaponized⁵ during the 2016 US election.

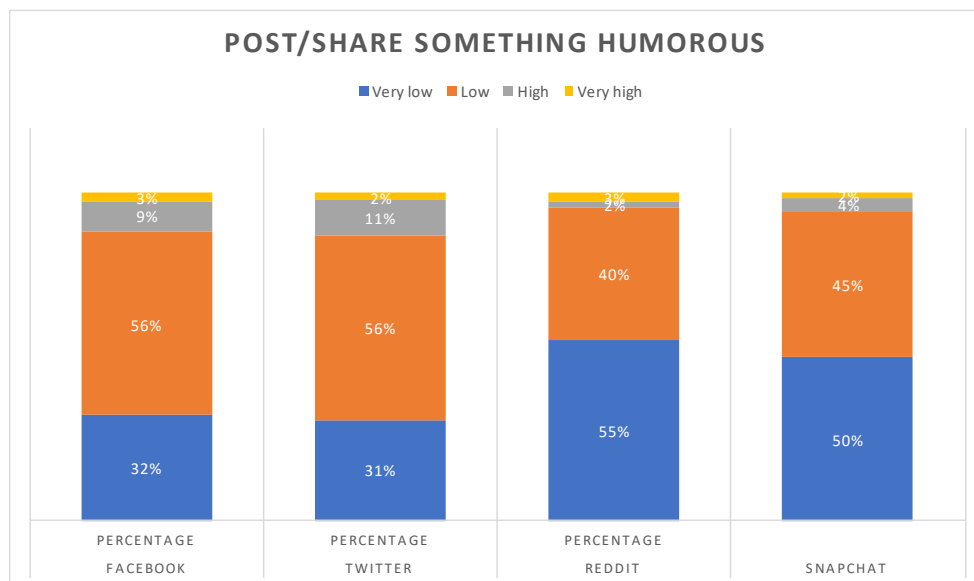


Figure 4.13: Shows how people perceive risk when posting/sharing humorous content on social media.

⁵<https://www.theguardian.com/us-news/2016/nov/04/political-memes-2016-election-hillary-clinton-donald-trump>

4.2.7 Participating in a debate

The perceived risk of participating in a debate can be seen in figure 4.14. From the figure, it seems like quite a lot of people perceive that participating in a debate on social media comes with high risk (15-40%) or very high risk (4-18%). Reddit here has the lowest perceived risk of the three social media users based on what was asked.

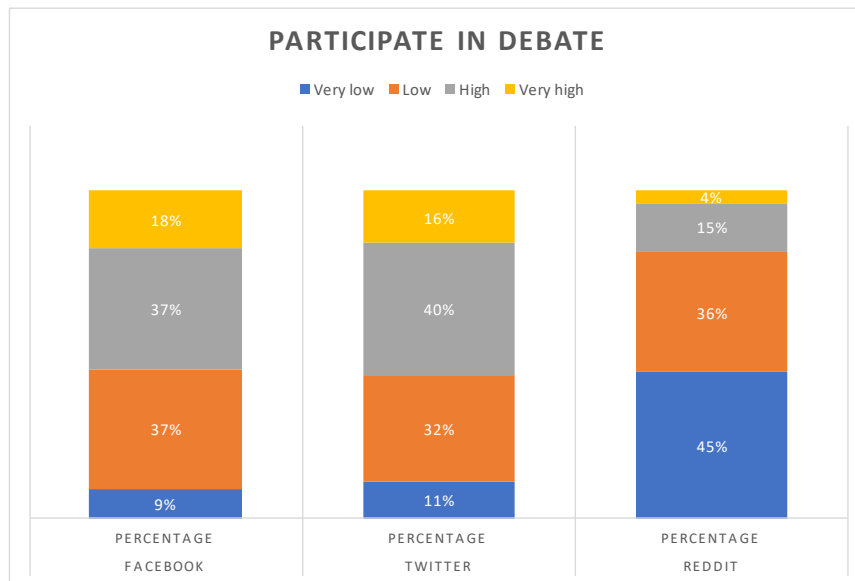


Figure 4.14: Shows how people perceive risk when participating in a debate on one a social media.

If we further examine the perceived risk of participating in a debate on social networks, we can see that some genders have a higher perceived risk than others. 4.15 doing an ANOVA analysis on genders and risk perception on debates on both Facebook and Twitter gives us a significance of 0.021. Reddit is a bit different here with just a significance of 0.096, see table 4.7. The gender group that had chosen “prefer not to answer” was taken out when performing the ANOVA because of the low number of respondents that chose this option, with only five people being in the group.

4.2.8 Use snapmap

Lastly, I asked how people perceive the risk when using Snapchat’s geographic location service Snapmap, figure 4.16. Snapmap shows on a map where users were the last time they used Snapchat if they have this service activated. Quite a lot of people that use Snapchat perceive snapmap as high risk (36%) or very high risk (26%). The questionnaire was running during late May, so the answers on perceived risk might have been influenced by the Norwegian state broadcast

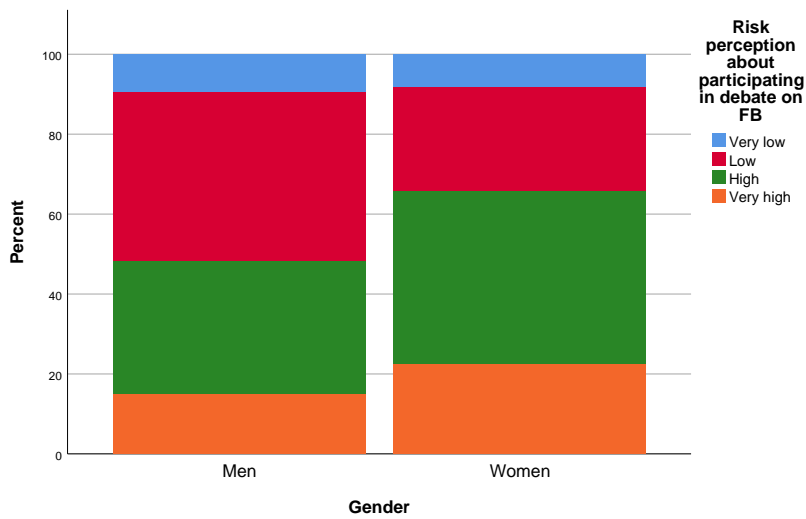


Figure 4.15: Shows how women and men perceive the risk of participating in debate on Facebook.

		Sum of Squares	df	Mean Square	F	Sig.
Debate on Facebook	Between Groups	4,053	1	4,053	5,372	0,021
	Within Groups	195,395	259	0,754		
	Total	199,448	260			
Debate on Twitter	Between Groups	4,104	1	4,104	5,423	0,021
	Within Groups	94,605	125	0,757		
	Total	98,709	126			
Debate on Reddit	Between Groups	1,974	1	1,974	2,825	0,096
	Within Groups	71,987	103	0,699		
	Total	73,962	104			

Table 4.7: Anova of genders and people participating in debate on social medias, excluding the gender "prefer not to answer".

Descriptives								
Participate in public debate Facebook								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Male	176	2,53	0,861	0,065	2,41	2,66	1	4
Female	85	2,8	0,884	0,096	2,61	2,99	1	4
Total	261	2,62	0,876	0,054	2,51	2,73	1	4

Table 4.8: Shows descriptives of genders and participating in public debate on Facebook, excluding the gender "prefer not to answer".

(NRK) article about private companies and surveillance ⁶.

⁶<https://www.nrk.no/norge/xl/avslort-av-mobilen-1.14911685>

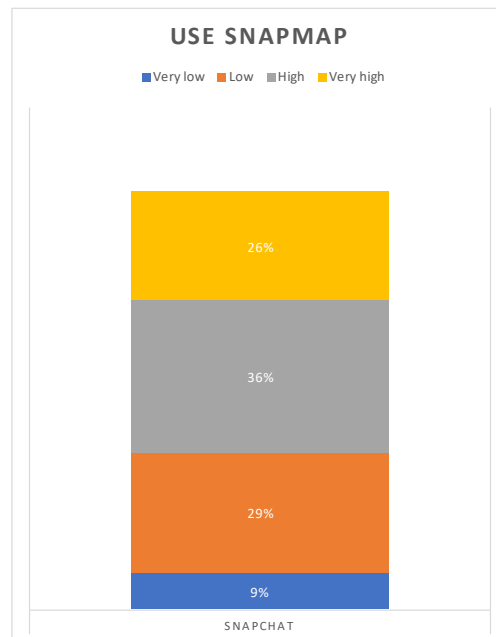


Figure 4.16: Shows how people perceive the risk of using Snapmap.

4.2.9 Posting/sharing and self-proclaimed privacy

If we look at the data where the respondents chose how much they care about IT, information security, and privacy. Doing a bivariate Pearson correlation analysis, we get that there is a correlation between most of the perceived risk when posting on social media, table 4.9. The correlation shows that if we define a weak correlation with everything above 0.3, there is a weak correlation with how many people say they care about privacy and how they perceive the risk when posting images on Facebook. In table 4.10 we can see that the people who said that they care a lot about privacy earlier in the questionnaire are also the ones that perceive the risk of posting on social media to be higher. The table with the numbers for how much people care about information security can be found in the appendix A.3

4.2.10 Changed privacy settings

In the questionnaire, the respondents were asked if they had changed their privacy settings. 301 people said that they had changed their privacy settings to reduce exposure, and 28 people had left them as is. In regards to the changing of privacy settings, I also asked to what degree that they had limited the visibility of their account N=329, figure 4.17. As can be seen in the figure, most people have limited the visibility of their information to a high degree. As can be seen from the figure, the one thing that people have tried to limit the most seems to be who can see their contacts, with about 84% of people rating their degree of limiting their contact visibility to 3 or 4. For all of the different privacy increasing measures that can

		IT generally	Information security	Privacy
IT generally	Pearson Correlation	1	,528**	,299**
	Sig. (2-tailed)		0	0
	N	329	329	329
Information security	Pearson Correlation	,528**	1	,645**
	Sig. (2-tailed)	0		0
	N	329	329	329
Privacy	Pearson Correlation	,299**	,645**	1
	Sig. (2-tailed)	0	0	
	N	329	329	329
Post image on FB	Pearson Correlation	0,107	,219**	,319**
	Sig. (2-tailed)	0,082	0	0
	N	265	265	265
Posting about vacation FB	Pearson Correlation	,127*	,252**	,257**
	Sig. (2-tailed)	0,04	0	0
	N	265	265	265
Posting image of pets with name FB	Pearson Correlation	,164**	,166**	,163**
	Sig. (2-tailed)	0,008	0,007	0,008
	N	265	265	265
Post/share news FB	Pearson Correlation	0,088	,207**	,218**
	Sig. (2-tailed)	0,153	0,001	0
	N	265	265	265
Post /share political FB	Pearson Correlation	0,092	,156*	,196**
	Sig. (2-tailed)	0,137	0,011	0,001
	N	265	265	265
Post/share humorous FB	Pearson Correlation	0,032	,151*	,170**
	Sig. (2-tailed)	0,599	0,014	0,005
	N	265	265	265
Participate in public debate FB	Pearson Correlation	0,064	,140*	,137*
	Sig. (2-tailed)	0,302	0,022	0,025
	N	265	265	265

Table 4.9: Shows Person correlation between how much the respondents care about IT, information security, privacy and the perceived risk when performing different actions on Facebook.

be done there seems that at the least 55% of people chose 3 or 4 as the degree that they had tried to limit visibility on their profiles, with stopping search engines from showing the profile as the least “important” one.

4.2.11 Visible information

The people who answered the questionnaire were asked what information they have visible on their social media platforms; the results can be seen in table 4.11. It seems like most people 58.5% have chosen to hide as much information about themselves as possible. As we can see, even though sexual orientation is classified as sensitive data according to Datatilsynet⁷ people still have this type of informa-

⁷<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/spesielt-om-sarlige-kategorier-av->

		Privacy							
		1		2		3		4	
		Count	Percentage	Count	Percentage	Count	Percentage	Count	Percentage
Post image on FB	Very low	1	33,30%	18	42,90%	19	16,80%	14	13,10%
	Low	2	66,70%	24	57,10%	75	66,40%	59	55,10%
	High	0	0,00%	0	0,00%	17	15,00%	28	26,20%
	Very high	0	0,00%	0	0,00%	2	1,80%	6	5,60%
Posting about vacation FB	Very low	1	33,30%	7	16,70%	2	1,80%	8	7,50%
	Low	2	66,70%	23	54,80%	62	54,90%	35	32,70%
	High	0	0,00%	10	23,80%	37	32,70%	42	39,30%
	Very high	0	0,00%	2	4,80%	12	10,60%	22	20,60%
Posting image of pets with name FB	Very low	2	66,70%	19	45,20%	33	29,20%	33	30,80%
	Low	1	33,30%	18	42,90%	68	60,20%	50	46,70%
	High	0	0,00%	5	11,90%	10	8,80%	17	15,90%
	Very high	0	0,00%	0	0,00%	2	1,80%	7	6,50%
Post/share news FB	Very low	1	33,30%	22	52,40%	34	30,10%	29	27,10%
	Low	1	33,30%	18	42,90%	67	59,30%	52	48,60%
	High	1	33,30%	2	4,80%	12	10,60%	21	19,60%
	Very high	0	0,00%	0	0,00%	0	0,00%	5	4,70%
Post /share political FB	Very low	1	33,30%	7	16,70%	10	8,80%	12	11,20%
	Low	1	33,30%	21	50,00%	60	53,10%	36	33,60%
	High	0	0,00%	14	33,30%	38	33,60%	41	38,30%
	Very high	1	33,30%	0	0,00%	5	4,40%	18	16,80%
Post/share humorous FB	Very low	1	33,30%	22	52,40%	33	29,20%	29	27,10%
	Low	1	33,30%	19	45,20%	66	58,40%	63	58,90%
	High	1	33,30%	1	2,40%	13	11,50%	9	8,40%
	Very high	0	0,00%	0	0,00%	1	0,90%	6	5,60%
Participate in public debate FB	Very low	0	0,00%	6	14,30%	8	7,10%	10	9,30%
	Low	1	33,30%	16	38,10%	49	43,40%	31	29,00%
	High	0	0,00%	18	42,90%	42	37,20%	37	34,60%
	Very high	2	66,70%	2	4,80%	14	12,40%	29	27,10%

Table 4.10: Shows how people post on Facebook, in comparison to how much they said they cared about privacy, where 1 caring little and 4 is caring a lot about privacy.

tion visible on their social media profile, in this case, 8.3% of the respondents.

Visible information	Count	Percentage
Email address	44	19.2 %
Home town	145	63.3 %
Phone number	26	11.4 %
Picture of me and my family	74	32.3 %
Political standing	15	6.8 %
Relationship	61	26.6 %
Family members	45	19.7 %
Sexual orientation	19	8.3 %
I don't have the clarity in it	35	15.3 %
Have hidden everything that I can	134	58.5 %

Table 4.11: Shows how many people have what kind of information visible and the percentage based on the number of total respondents on the questionnaire 329.

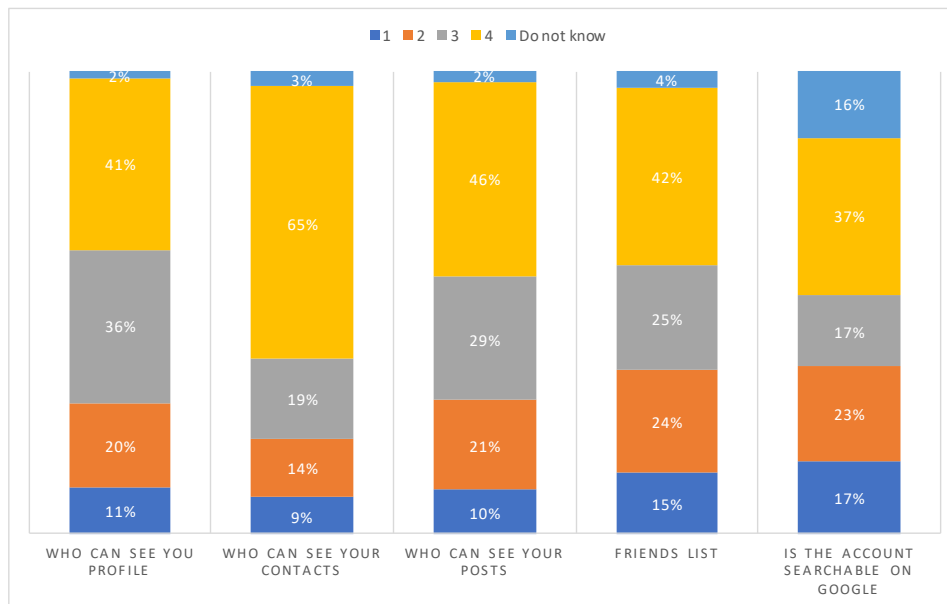


Figure 4.17: Asked to what degree they had limited the different kinds of information visibility, where 1 is that they have limited the visibility of the information minimally and 4 is that the visibility of the information has been limited greatly.

4.2.12 Perception on what can be used in performing ID-theft

The participants in the questionnaire were asked how they rate 10 different kinds of information, and to what degree they thought that the information could be used to perform identity theft. The results can be seen in table 4.12. The one piece of information that would people thought would let an attacker perform an ID-theft was Account and password details with 80.9% of people rating it as greatly. In second place we have debit/credit card numbers with 77.4% on greatly when I asked this question I was just considering the front-facing numbers, but people might have thought I meant all the numbers on the card. We can see that over around 66 % of people perceive social security numbers as a greatly in regards to the information risk value, even though the social security number is not classified as sensitive data, and should in theory, not let people take up loans in your name. How people rated the rest of the information points asked can be seen in table 4.12.

Doing an ANOVA test on the digital natives and non-digital natives we can see that there is a statistical significance in how they perceive the risk with their date of birth in regards to an attacker that wants to perform identity theft, table 4.13. We can see the difference in figure 4.18, and here we can see that it is the digital natives that perceive the risk of their date of birth being easily found out, and to what degree it can be used to perform ID-theft.

Information	Answer	Count	Percentage
Full name	Minimal	45	13.70 %
	Slightly	156	47.60 %
	Moderately	89	27.10 %
	Greatly	38	11.60 %
Phone number	Minimal	35	10.70 %
	Slightly	122	37.20 %
	Moderately	123	37.50 %
	Greatly	48	14.60 %
Email	Minimal	33	10.10 %
	Slightly	128	39.10 %
	Moderately	116	35.50 %
	Greatly	50	15.30 %
Social security number	Minimal	20	6.10 %
	Slightly	26	7.90 %
	Moderately	65	19.80 %
	Greatly	218	66.30 %
Date of birth	Minimal	28	8.50 %
	Slightly	127	38.70 %
	Moderately	120	36.60 %
	Greatly	53	16.20 %
Home address	Minimal	28	8.50 %
	Slightly	139	42.40 %
	Moderately	108	32.90 %
	Greatly	53	16.20 %
Account number	Minimal	32	9.80 %
	Slightly	49	15.00 %
	Moderately	69	21.10 %
	Greatly	177	54.10 %
Debit/credit card number	Minimal	20	6.10 %
	Slightly	12	3.70 %
	Moderately	42	12.80 %
	Greatly	254	77.40 %
Health data	Minimal	25	7.60 %
	Slightly	86	26.20 %
	Moderately	95	29.00 %
	Greatly	122	37.20 %
Account info and password	Minimal	11	3.30 %
	Slightly	17	5.20 %
	Moderately	35	10.60 %
	Greatly	266	80.90 %

Table 4.12: People were asked to rate to what degree they thought the different information could be used in performing ID-theft. The question asked was: To what degree to you think this information can be used against you to perform an identity theft against you? N=327-329(some people did not answer every question)

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	6,893	1	6,893	9,62	0,002
Within Groups	233,583	326	0,717		
Total	240,476	327			

Table 4.13: Anova between digital natives and non-digital natives seeing if there is a difference in how they perceive the risk with date of birth.

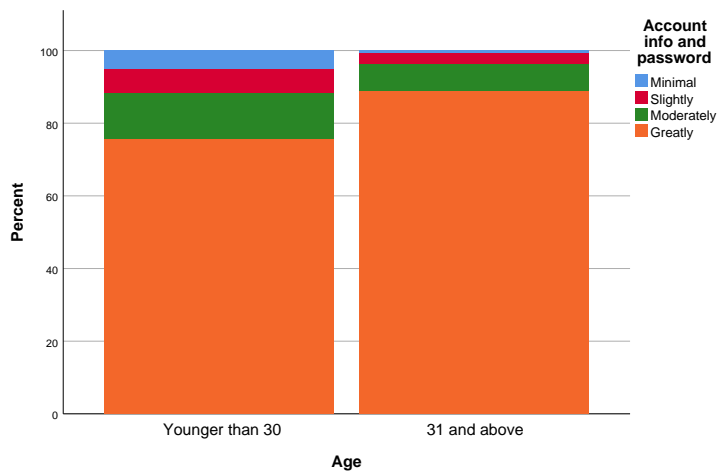


Figure 4.18: Comparison of how digital natives and non-natives rate to what degree their date of birth can be used in identity theft, represented in %, for the different age groups.

Another ANOVA analysis on digital natives and non-digital natives and the degree to which they believe that debit/credit card numbers can be used in performing identity theft shows that there is a significant difference sig=0.004 between the group's table 4.14. The differences in the answers can be seen in figure 4.19, and it shows that the digital natives about 9% think that there is minimal that can be done if someone knows their debit/credit card numbers.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5,436	1	5,436	8,198	0,004
Within Groups	216,161	326	0,663		
Total	221,598	327			

Table 4.14: Anova between digital natives and non-digital natives seeing if there is a difference in how they perceive the risk with debit/credit card numbers.

Again we can do an ANOVA analysis, but here we compare the answers of Digital natives and non-digital natives with their ratings on how useful passwords are in performing Identity theft, see table 4.15. I found that digital natives believe

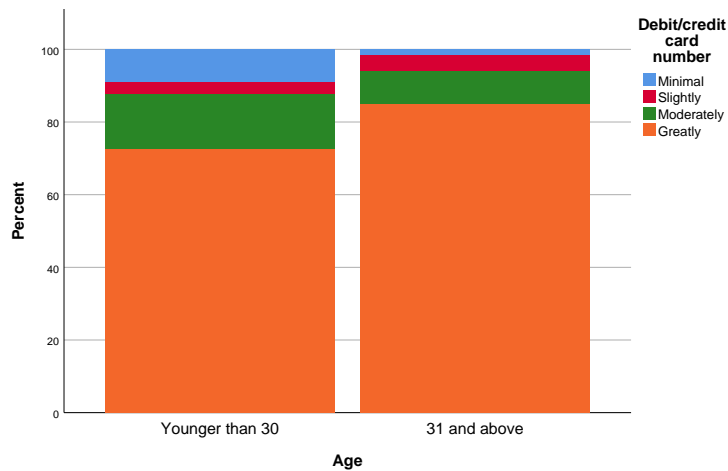


Figure 4.19: Comparison of how digital natives and non-natives rate to what degree their debit/credit card numbers can be used in an identity theft, represented in %, for the different age groups.

that account information and passwords help an attacker to a lesser degree than what non-digital natives believe, see figure 4.20. We can see that around 10 % of the digital natives find the perceive the risk to be slight or lower.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5.022	1	5.022	9.932	0.002
Within Groups	165.355	327	0.506		
Total	170.377	328			

Table 4.15: Anova between digital natives and non-digital natives seeing if there is a difference in how they rate account info and passwords.

4.3 Compromised social media accounts

There are many ways to use a hacked social media account. From the questionnaires distributed, the number of people that have experienced being hacked can be seen in table 4.16. As we can see from table 14.3 % of the respondents of the questionnaire have been hacked and gotten their accounts back, 0.9 % has been hacked and have not gotten their account back, and 84.8 % of people have not experienced having their account on social media compromised. The respondents that had experienced being hacked got some further questions about their experiences from having their accounts compromised.

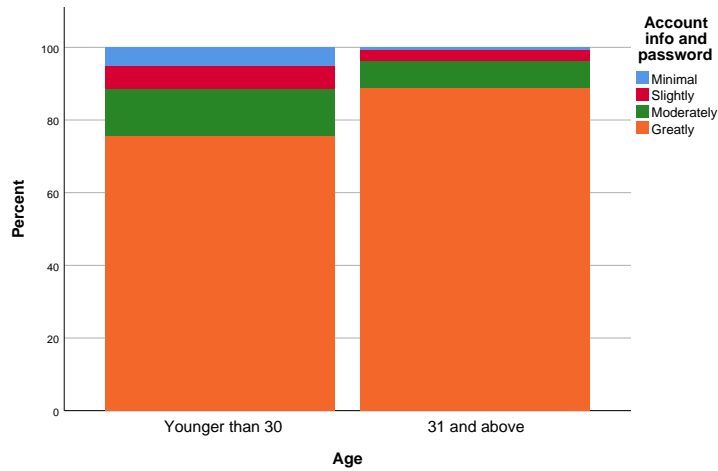


Figure 4.20: Comparison of how digital natives and non-natives rate to what degree their account and passwords can be used in an identity theft, represented in %, for the different age groups.

		count	Percentage
Have you been hacked?	Yes	47	14.30 %
	No	279	84.80 %
	Yes, but I have yet to receive my account back	3	0.90 %
	Total	329	100.00 %

Table 4.16: Shows the number of people who has had their account hacked.

4.3.1 Reason for compromise

The table 4.17 shows what people thought were their reasons for compromise N=47. The hacked option might be a bit too broad, and the answers might have just as well been placed in the do not know option; it is hard to know if the reason to compromise is the reuse of a password or a weakness in the platform used. We can see from the numbers that eight people, or about 17 % of the people that had their accounts compromised, had their accounts compromised because of some phishing scheme. For the people who chose other, one had their account compromised by a Keylogger, one had Bruteforcing, and the last one attributed the hacked account either to a keylogger or a remote access tool.

4.3.2 Consequences of social media ID theft

What the respondents had as consequences can be seen in table 4.18 as one can see, many people have not been able to attribute or find out exactly why their account was hacked. People had difficulties attributing what their social media

Believed reasons of compromise	Count
Phishing	8
Shared the password with someone I have relations with	2
Hacked	15
Other	3
No/don't know	19

Table 4.17: Shows peoples answers on what they thought were their reasons of compromise N=47.

account were used for when hacked. When they managed to attribute what the hackers did, it was usually because they used the account for spam or phishing. The respondents in this open answers question gave mostly just one consequence that the hackers ended up using the account for, and as we can see from the figure about 65 % do not know or have not experienced any consequences of having their account compromised, meaning that around 4% of the population overall has their accounts compromised and experience some kind of consequence. 10% of people experienced the consequence that their account was used to send out spam messages. 8% of people had the account send out phishing messages or that the account was used in other phishing campaigns. 5% experienced blackmail from the compromise; the hacked account contains much personal information, especially if one uses the social media as their primary chatting application, which an attacker can use to blackmail the owner of an account. The rest of the consequences can be seen in table 4.18

Consequence	Count	Percentage
No known consequence	26	65 %
Spam	4	10 %
Phishing	3	8 %
Blackmail	2	5 %
Link sharing	1	3 %
Account deleted	1	3 %
Lost permanent access	1	3 %
Used to increase follower count	1	3 %
Malware	1	3 %

Table 4.18: Shows categorised reasons for compromise from text answer in the questionnaire. The reasons have been grouped a bit together with other similar consequences N=47.

The people who answered that they had not experienced having their social media profile hacked, were asked in a question with an open answer field what

they thought a compromised social media account could be used. The answers that they gave have been grouped up with common characteristics like extortion and blackmail would just be placed as blackmail in the analysis, the groups ended up being pretty broad to try place the open answers people gave, some people talked about multiple uses for their account and the counts for all the uses of compromise mentioned was incremented. The answers can be seen in table 4.19. I was also looking for keywords in their answers and paired those into categories; for example, *pretending to be* or *impersonation* would be placed into the impersonation/ID-theft category, and if they mention *spam* or *commercial* they would simultaneously also be placed into spam. The thinking here was that the attacker compromised the account to misuse the trust other people had with the owner of the account, to have them click links or buy bad products. There are 197 in total for the table; this is because not everyone answered with any thoughts.

Uses for a compromised account	Count
Impersonation/ID-theft	40
Spam	26
Spread malware	23
Phishing	18
Manipulation	17
Steal money/swindle	15
Blackmail	14
Destroy reputation	14
Nothing/little	12
Misuse of content on the platform	11
Don't know	8
Follower farming	4
Gain access to other things	3

Table 4.19: Grouped open answers for that a compromised account can be used for. N=329 with around 60 answers being blank or not relevant.

4.3.3 Activated measures

The respondents who had had their social media account compromised were asked what kind of measures they had implemented to increase the security of their account, the controls implemented can be seen in table 4.20. The question about measures implemented let them choose more than one option; that is why the total number of controls exceeds the N=47 people who had their accounts compromised. Not all the security measures I asked about are current best practices in information security like periodic password changes, that NIST is now not recommending companies to require[38]. From table 4.20, we can see that the most popular measure to apply is 2-factor authentication 32, and notification on suspicious behavior 29. After that comes starting to use passwords longer than 12

characters 22 and having the firewall turned on 15. 13 people started changing their passwords regularly, 11 started using an anti-virus, and nine people took other measures. 5 People have changed their passwords to a password shorter than 12 characters.

Measures	Count
Activated 2 factor authentication	32
Activated notification on suspicious behavior from the account	29
Changed password to a password 12 characters or longer	22
Have the firewall turned on	15
Stared changing passwords regularly	13
Use anti-virus	11
Other	9
Changed password to a password shorter than 12 characters	5

Table 4.20: Measures users who have had their accounts compromised have activated to help mitigate a new compromise. N=47

The people that chose the option that they were changing their password regularly were asked with what regularity they change their passwords. From the table 4.21, we can see that most of the people who have decided to incorporate regular password changes into their security practices choose to change their passwords every third month. Seven people decided to start changing their passwords every third month, while three people decided that once a month was the appropriate time for regular changes. One person went with more frequently than once a month; one person went with every six months, and one person changes their password yearly.

Password change frequency	Count
Every third month	7
Every month	3
More frequent than once a month	1
Every six months	1
Every year	1
More infrequent than every year	0

Table 4.21: Shows how often the people who had decided to use regular password changes as a control changes their passwords. N=13

4.3.4 Would people click a possible phishing link

The table 4.22 shows how people would react on a phishing message received from a *. The message that was shown to the respondents can be seen as figure 4.21. This shows that this type of phishing can be expected to get between 8 % and 15 % hit rate of people clicking these kinds of links. With 6.1 % of people saying they might click the link if it is sent from close family, it is 4.1



Figure 4.21: Example message that has been circulating from hacked Facebook accounts and sent to people on their friends list. <https://nettrett.no/falske-videomeldinger-i-messenger/>

	Answer	Count	Percentage
Acquaintance	Yes	4	1.30%
	No	289	92.00%
	Maybe	21	6.70%
Friend	Yes	13	4.10%
	No	269	85.70%
	Maybe	32	10.20%
Family	Yes	13	4.10%
	No	275	87.60%
	Maybe	26	8.30%
Close family	Yes	19	6.10%
	No	264	84.10%
	Maybe	31	9.90%

Table 4.22: Who the respondents thought they might get tricked into clicking a link if they received it from. N=314

4.3.5 Insight form interviews

In the Slettmeg questionnaire, the respondents were asked if they were open for some further contact if there was anything extra that could be interesting to explore. I contacted two people who had their accounts compromised; I tried to get in contact with five, but only two people replied.

One of the people I contacted had tried to figure out more about how they got compromised. They had two main hypotheses for how the Facebook account got compromised. One was that they had gotten phished and led to a landing page that looked identical to the Facebook login page. Hypothesis number two was that they had an old .live address taken over by a hacker. They had gotten in contact with Microsoft and the person they talked with confirmed that the email had been deleted due to inactivity and that it had been given to someone new⁸. This account was then used to try to gain access to a business account and buy ads on Facebook. They regained access to their account again after quite a while back and forth with Facebook. I asked if they had any final thoughts on what happened and how the compromise felt.

I asked the other person whom I got in contact with whether they knew how their account was compromised, they thought it might have been because they had clicked a link, whether this link downloaded malware or was used for phishing, they did not know. They got informed that their account had been compromised when the account started sending out spam posts on their wall advertising ray bans or knock offs, and they were informed by some friends who also reported the profile as hacked to Facebook. Because the account was reported as hacked, Facebook quickly secured the account and stopped the hackers from using it any further.

I asked both of the people who agreed with a short interview how they felt about the situation and whether they had any thoughts about the event now after the fact. They both said that it felt like a severe violation of their privacy and personal sphere. Both people were non-digital natives and with the paper from Golladay and Holtfreter [21], they found that older people have a stronger emotional response from experiencing identity theft. Sadly I did not get any data from any digital natives about how they felt about the situation after the fact.

⁸Microsoft and Yahoo has had a tendency of reusing email addresses, which has given hackers an opportunity of picking them up and getting into accounts associated with the email. <https://www.pcworld.com/article/2052586/microsoft-is-quietly-recycling-outlook-email-accounts.html>

Chapter 5

Discussion

The discussion chapter takes the original research questions and explores them further by discussing the questionnaire and the results from the analyzed questionnaire. This section is set up to follow the same order as the research questions.

1. What is the state-of-the-art approach for researching risk perception of ID theft?
2. What are the known consequences of social media ID theft in Norway?
3. How do people perceive the risk of ID theft on social media?
4. What data do people believe can be used by a possible attacker?
5. Do privacy concerns impact sharing habits?

5.1 Research question 1: What is the state-of-the-art approach for researching risk perception of ID theft?

To answer my first research question, which was done with a literature review, there seems to be a myriad of ways to measure risk perception. One of the ways was to do what I did and use a questionnaire. A lot of the different ways also wanted one to do more qualitative research, but because of the time constraints and the Coronavirus that during the thesis writing making a more qualitative approach difficult, most of this thesis is based on quantitative analysis and data. It would probably have been advantageous to do more qualitative research as well during this thesis. Being able to talk to more people about their thoughts on research questions 3 and 4, the questions I asked seemed to in hindsight to maybe not hit the questions, as well as I would have liked. Showing that being able to do more qualitative research here could have been advantageous, and strengthening what I saw when doing my literature review should combine qualitative and quantitative methods when researching risk perception.

5.2 Research question 2: What are the known consequences of social media ID theft in Norway

There are a lot of different things compromised social media accounts can be used for, as can be seen in table 4.18, using a social media account to send out spam messages is probably a way for a hacker to try to exploit the trust between the two parties, the hacked account and the person receiving the spam message or the person who sees the spam post. This is a form of impersonation of the person who had their account hacked. Most of the known consequences that the people who had their accounts hacked are where links were shared, either with malware, phishing, or spam. I also found out from the talk I had with one of the people who was compromised that the hacker used their business account on social media to buy ad slots on the platform. There can be big money in it for hackers ¹. A couple of people found their accounts to be inaccessible after they got hacked, it is probably challenging to ascertain whether it was the social media platform that deleted or closed down their account, because of suspicious behavior, or if it was the hackers that were performing some denial of service.

5.2.1 Value of information

There are multiple ways one can put a value on information; one can ask people what their information is worth like Trend micro did in a survey², or one can see what the different types of information are going for on the dark web.

The information in table 4.12 shows how people value their information in regards to what can be used in performing identity theft. We can compare some of this data with a trend micro survey, where they asked respondents how much they thought their information was worth in a dollar value. The top 5 most valued information they found were:

1. Passwords with the value of \$75.80c
2. Health information with an average value of \$59.80 and \$35 from European consumers.
3. Social security number \$55.70
4. Payment details at \$36.60 on average and \$20.70 in Europe
5. Purchasing history \$20.60

They found that passwords had the most value at 75.8 dollars, this seems consistent with the answers from the questionnaire with the account details and password being the data that the respondents perceived as most likely to help an attacker perform a successful identity theft. The following information the Trend micro respondents put the most value in was Health data, if we compare that with the table 4.12 We can see that health data has a pretty high score here too, but

¹<https://www.cnet.com/news/your-hacked-facebook-account-may-be-bankrolling-scam-ad-campaigns/>

²<https://www.trendmicro.com/vinfo/tr/security/news/internet-of-things/how-much-is-your-personal-data-worth-survey-says>

that there are other information that people perceive as being more useful in performing Identity theft. In a paper written by Vargas [9], he found that there is a significant and living market on the dark web for our personal information. He found that a hacked Facebook account was worth around 5 dollars, and if a hacker downloaded and sold all the information readily available from the “GDPR download personal information” you could get even more money from a compromised social media account.

5.3 Research question 3: How do people perceive the risk of ID theft on social media?

To answer this question I asked the respondents of the questionnaire, what information they thought could be used against them in performing identity theft, I also asked people what they thought were the consequences for a compromised account on social media. These questions together were designed to give some inkling what people thought a compromised account could be used for, and give a bit information on how easy people might think compromising an account might be. We can see that if we keep in mind what information people have visible, and look at what people believe that could assist in ID theft, that around 19% has their email address visible, while around 50 % judge email address to moderately or greatly to be able to assist in ID theft.

The consequences people who have had their accounts compromised matches pretty well up with what people in this study believe a compromised account can lead to. Most people mentioned that impersonation/ID-theft in their answers for what consequences for a compromised account could be and how the compromised could be used to send out things like spam or malware misusing people’s trust. Looking at the table 4.19, we can see from what people answered what they perceive as the most significant risks with having their accounts compromised. The table shows that people believe that some form of impersonation ID theft with the account is the primary consequence of a compromised account and that this account will, in turn, be used for some form of spam, phishing, etc. It is also interesting how 17 people mentioned manipulation in their answers, with how different state actors try to manipulate the democratic processes around the world, it is a great risk to keep in mind. We saw in Norway NRK having a program on election manipulation on a school in Lillestrøm, they did not think their efforts worked as well as they thought they would, but there might have been a small change in the voters³.

All in all, there does not seem like there is one way people perceive the risk of ID theft on social media; the answers vary substantially independent of demographic data. There were two significant outliers that people perceived differently one was between digital natives and non-natives that perceived their date of birth

³<https://www.nrk.no/norge/folkeopplysningen-forsokte-a-manipulere-skolevalg-1.14686244>

differently to what degree it could be used in ID theft, debit/credit card numbers, and account credentials. The other one was between males and females in table A.9, which shows that email, birth date, and account numbers have a significant difference. So there are some differences between different demographics.

5.4 Research question 4: What data do people believe can be used by a possible attacker?

From table 4.11, We can see what information people have readily available on their profiles. There is a lot of information people have available on their profile that can assist in performing identity theft. For example, having emails and passwords might let an attacker spoof (pretend) that they are the contact information's owner. Showing family members might be a way for an attacker to figure out whom they should focus on when trying to send phishing messages trying to swindle money. If people have a lot of this information posted on their profile, it might be easier for an attacker to gain credibility when talking to other parties than just family.

The table 4.12 shows more directly what data the people who answered the questionnaire could be used to perform identity theft. Showing that the user credentials are the data that people are most concerned about when it comes to identity theft. If we look at the data in table 4.12, that is information that is more usual to have public, we can see that people rate home address, date of birth, and email as some of the more important ones. It is difficult to rate how much some of the information can assist in practice with performing identity theft; the problem is usually the magnitude of available information and this information put into perspective by an attacker, that lets an attacker perform a social engineering attack to gain something from the victim.

5.5 Research question 5: Does privacy concerns impact sharing habits?

For the most part, there are minimal differences in what people share on social media, age, and gender mostly does not have any significant impact on what we share. The only big outlier when it comes to sharing or putting themselves more "out there" is when people participate in a debate. When participating in a debate, we saw that women perceive the risk as higher men's, table 4.7. There was also quite a big difference in how people or what people utilize Reddit compared to the other types of social media, with people from Reddit having a much lower perceived risk when participating in debate, figure 4.14. This might also come from there being fewer women who use Reddit with most of the gender on Reddit from the questionnaire being male, figure 4.1.

The high-risk perception for participating in a debate might have a connection with why most people in online debates have a firm standpoint, people who

are more centralist perceive the risk as too high compared to what they want to convey. If there is a connection between the perceived risk and people feeling the risk of participating is too high, then this might be a societal issue where we end up splitting the population more and more into two groups. Interestingly, the risk perception of participating in debate is so high compared to that of sharing/posting news stories (figure 4.11) with all we hear about fake news in media. If we look at these answers and compare them to the results from Warner-Sønderholm et al.[31] where they found that people more easily trust what shows up in their news feed on social media. We can see why this might create a negative feedback loop where fake news gets spread because people do not see sharing them as a risk. Furthermore, people have a higher tendency to believe in what shows up in their feed. One might also think that if people end up posting what Trump has coined as *Fake News* that this could damage a person's reputation.

When it comes to what people share on social media as information about them, to people outside their circle of trust - their group of friends, we saw that most people had tried to at least to a high degree limiting the visibility on their profiles, see figure 4.17. Moreover, we can also see from table 4.11 that people seem to have removed or decided not to have a lot of information open publicly on their social media profiles, with their home town being the thing most people display at 63%. The information displayed on the profile is set to public by default on Facebook unless one changes who can see their information.

In table 4.9, we saw that there is a weak correlation between people's privacy and if they post images on Facebook. There can be multiple reasons as to why people see posting images on Facebook as a privacy concern. The concern might stem from people not wanting pictures with metadata[37] being on Facebook; it can also stem from peoples growing concern regarding *Big brother state* where pictures can be used in machine learning to pick people out from crowds and increase surveillance on people.

Chapter 6

Limitations and future work

Some things could have gone better during the master thesis, and some findings could be interesting to explore more. This section will explore the limitations of the study and what could be interesting to look at for future works.

6.1 limitations

In this section, I will explore some of the limitations I have found in my questionnaire and how I decided to construct/manage my thesis.

6.1.1 Data gathering

When performing the data gathering for the study, the original plan was to gather data only by asking people who contacted Slettmeg.no during a month. When it was clear that only using Slettmeg as the only source of recruitment for the questionnaire would not give enough respondents the sampling, a decision was made to try sampling broader. Due to time restraints during the end of the thesis, the recruitment of new respondents ended up becoming a convenience sampling. With this convenience sampling, I also gained a quite skewed demographic view, with mostly males answering, mostly people from Oppland and Oslo. The data gathering through social media also made sample control challenging to accomplish, with, for example, how there was no way of knowing how many people in actuality saw the posts that tried to recruit people into the questionnaire. With the mostly passive participant recruitment, it was also difficult to recruit people from demography that lacked participation compared to Norway's population.

There were also some small hiccups during the data gathering, where I had set some questions to allow multiple answers, where they should have been single answer questions, this was noticed pretty early in the data gathering when the questionnaire was placed on Facebook, but when I changed the variable into becoming a single choice, I lost 16 answers on the affected questions.

6.1.2 Feedback from the questionnaire

I received some feedback that some of the questions were confusing in how the questions were worded. That, combined with how they were combined with the Likert scale with 1-4, could confuse. One of the questions that I can see could have been difficult, with this in mind is the question where I asked how much people had tried to limit their public data. The question here is not super intuitive, but I ended up wording it as I did to make it general enough for it to apply to all social media platforms instead of making it, for example, Facebook-specific with taking the different privacy settings from there. A commentator also commented that I should have added an alternative for people who do not post on social media, the problem with adding that is that, that might have skewed the people who believe the social media to be high risk might have just defaulted to the answer that they never post without thinking of the reason as to why they do not post. I should probably have added a sentence at these questions asking people to rate how they thought the risk would be if they post the following information. Another comment received from multiple people was that I should have ended the questionnaire with the demographic questions to increase the retention of people and have them more fully focused on the questionnaire when they answered the difficult/important questions.

6.2 Future work

To better gauge why people feel that social media is less risky than another, asking people to rate how anonymous they find the given social media could have been an interesting data point that could have shone some more light on why somethings are perceived as less risky than other. This data point might have given some insight into why some social media platforms perceive the risk of posting/sharing as lower than others. Doing a bivariate correlation between the same types of data and the differences in platforms showed that people generally chose the same options regardless of which platform they were asked about, see table A.7. The differences between the different social media platforms might stem from who uses the platforms, with how they answered, for the most part, the same things on the different social media. The main difference in the social media answers seemed mostly to stem from where the respondents were recruited from independent on what platforms they use, this might have a connection with what platforms they primarily use, but I had no questions to ascertain if there is some connection there.

Another data point that could be interesting to explore more is trying to figure out if some social media accounts are being used for different things than the others. For example, are most Twitter accounts used to mass follow different accounts, or are they mostly used to spread propaganda if the user has many followers. Another big reason to hack a Facebook account to be able to buy ads to spam people, or is it the main thing hackers try to do is send out spam/phishing messages to people.

Another thing that could be interesting to do some future research on is if and how risk perception limits how much people are willing to say their opinion in a matter where they have a more moderate opinion. Seeing that the consequence of participation is higher than the reward. How much does the perceived risk stifle them from saying their opinion, and is there any way to reduce this high perception of risk to make for a healthier debate climate?

It could have been interesting to ask people if they knew what their accounts were being used for while it was hacked. I tried getting insight into this with my question about consequences, but if the account had a more *hostile takeover*, where the name and picture got changed to phish or gain *street cred* these consequences can have slipped peoples mind because the consequences were not necessarily connected to them anymore. One of the reasons this was not asked in the questionnaire was the time limitation, where I did not want the questionnaire to be too long for people as not to make them lose interest in completing the questionnaire.

Chapter 7

Conclusion

Social media is not just an excellent platform to help us stay interconnected to old family members and friends; it can also be used by attackers or people with less than honest ambitions trying to exploit people. The conclusion is also constructed around the research questions, giving a conclusion to what I found out during this thesis.

Research question 1: What is the state-of-the-art approach for researching risk perception of ID theft? Risk perception seems to be a highly individual thing. To measure risk perception accurately, one should, as the literature review showed, use more of a combined approach between quantitative and qualitative approaches to get a better understanding of what people put into their perception of risk, what are the consequences that they perceive.

Research question 2: What are the known consequences of social media ID theft in Norway? There are many possible consequences that can happen if one has their social media account compromised. The primary consequence found in my questionnaire of being hacked was that their account was used to distribute spam and phishing messages, this shows that the most lucrative approach for hackers seems to be to misuse the identity and trust of the hacked accounts. We also saw that around 14% of the population has experienced having their social media accounts compromised, with 65% not seeing any consequence from the compromise, giving us that around 4% of the population will have their accounts compromised and have known consequences.

Research question 3: How do people perceive the risk of ID theft on social media? The belief people have regarding ID theft on social media seems to fit well with what people who have experienced having their accounts compromised. Many hackers are trying to leverage the hacked accounts identity to spread spam or phishing links out into the hacked accounts social circle.

Research question 4: What data do people believe can be used by a possible attacker? When it comes to people's perceived riskiest information in aiding in identity theft, account credentials was rated the highest with around 80.9% of people rating it as greatly, on place number two we had debit/credit card number with 77.%, followed by social security numbers at 66.3%. With the information that is more common to have public Home address and date of birth are tied with 16.2% on greatly.

Research question 5: Do privacy concerns impact sharing habits? There was a weak correlation with what people share when compared with their focus on privacy and information security, and that was when people share images on Facebook, and we compare this to privacy. I also found that women have a look at participation in public discourse on social media, as riskier than what men perceive it as. Most people also have in regards to their privacy decided to, to some degree, limiting the visibility of what can be seen on their profile or how easy it is to find the profile.

To conclude more in general terms, people seem to be aware of quite many of the risks that a compromised account on social media can mean, and people perceive the risk of doing things on social media very differently. Older people (non-native) seem to perceive some risks as higher than the digital natives. And lastly people should consider activating two factor authentication, which for the most part removes the risk of being hacked.

Bibliography

- [1] N. Gerber, B. Reinheimer and M. Volkamer, 'Investigating people's privacy risk perception', *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 3, pp. 267–288, 2019. [Online]. Available: <https://content.sciendo.com/view/journals/popets/2019/3/article-p267.xml>.
- [2] N. H. A. Rahim, S. Hamid, M. L. Mat Kiah, S. Shamshirband and S. Furnell, 'A systematic review of approaches to assessing cybersecurity awareness', eng, *Kybernetes*, vol. 44, no. 4, pp. 606–622, 2015, ISSN: 0368-492X.
- [3] S. Furnell, P. Bryant and A. Phippen, 'Assessing the security perceptions of personal internet users', eng, *Computers & Security*, vol. 26, no. 5, pp. 410–417, 2007, ISSN: 0167-4048.
- [4] S. Talib, N. Clarke and S. Furnell, 'An analysis of information security awareness within home and work environments', eng, in *2010 International Conference on Availability, Reliability and Security*, IEEE, 2010, pp. 196–203, ISBN: 9781424458790.
- [5] E. Kritzinger and S. Von Solms, 'Cyber security for home users: A new way of protection through awareness enforcement', eng, *Computers & Security*, vol. 29, no. 8, pp. 840–847, 2010, ISSN: 0167-4048.
- [6] W. A. Labuschagne, N. Veerasamy, I. Burke and M. M. Eloff, 'Design of cyber security awareness game utilizing a social media framework', eng, in *2011 Information Security for South Africa*, IEEE, 2011, pp. 1–9, ISBN: 9781457714832.
- [7] A. Marcon, G. Nguyen, M. Rava, M. Braggion, M. Grassi and M. E. Zanolin, 'A score for measuring health risk perception in environmental surveys', *Science of The Total Environment*, vol. 527-528, pp. 270–278, 2015, ISSN: 0048-9697. DOI: <https://doi.org/10.1016/j.scitotenv.2015.04.110>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0048969715300449>.
- [8] W. He, 'A review of social media security risks and mitigation techniques', *Journal of Systems and Information Technology*, vol. 14, Apr. 2012. DOI: 10.1108/13287261211232180.

- [9] V.-M. Vargas, 'The new economic good: Your own personal data. an integrative analysis of the dark web', in *Proceedings of the International Conference on Business Excellence*, Sciendo, vol. 13, 2019, pp. 1216–1226.
- [10] P. Slovic, B. Fischhoff and S. Lichtenstein, 'Facts and fears: Understanding perceived risk', in *Societal risk assessment*, Springer, 1980, pp. 181–216.
- [11] A. S. Alhakami and P. Slovic, 'A psychological study of the inverse relationship between perceived risk and perceived benefit', *Risk analysis*, vol. 14, no. 6, pp. 1085–1096, 1994.
- [12] P. Slovic, 'Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield', *Risk analysis*, vol. 19, no. 4, pp. 689–701, 1999.
- [13] 'Information technology - security techniques - information security risk management iso27005:2008', British Standard, Tech. Rep., 2008.
- [14] P. Slovic, M. L. Finucane, E. Peters and D. G. MacGregor, 'Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality', *Risk Analysis*, vol. 24, no. 2, pp. 311–322, 2004. DOI: 10.1111/j.0272-4332.2004.00433.x. eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.0272-4332.2004.00433.x>. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.0272-4332.2004.00433.x>.
- [15] G. F. Loewenstein, E. U. Weber, C. K. Hsee and N. Welch, 'Risk as feelings.', *Psychological bulletin*, vol. 127, no. 2, p. 267, 2001.
- [16] K. Bickerstaff, 'Risk perception research: Socio-cultural perspectives on the public experience of air pollution', *Environment International*, vol. 30, no. 6, pp. 827–840, 2004, ISSN: 0160-4120. DOI: <https://doi.org/10.1016/j.envint.2003.12.001>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0160412003002472>.
- [17] A. Hedayati, 'An analysis of identity theft: Motives, related frauds, techniques and prevention', *Journal of Law and Conflict Resolution*, vol. 4, no. 1, pp. 1–12, 2012.
- [18] F. Lai, D. Li and C.-T. Hsieh, 'Fighting identity theft: The coping perspective', *eng, Decision Support Systems*, vol. 52, no. 2, pp. 353–363, 2012, ISSN: 0167-9236.
- [19] G. R. MILNE, A. J. ROHM and S. BAHL, 'Consumers' Protection of Online Privacy and Identity', *Journal of Consumer Affairs*, vol. 38, no. 2, pp. 217–232, Jan. 2004, ISSN: 1745-6606. DOI: 10.1111/j.1745-6606.2004.tb00865.x. [Online]. Available: <https://doi.org/10.1111/j.1745-6606.2004.tb00865.x>.

- [20] K. B. Anderson, 'Who are the victims of identity theft? the effect of demographics', *Journal of Public Policy & Marketing*, vol. 25, no. 2, pp. 160–171, 2006. DOI: 10.1509/jppm.25.2.160. eprint: <https://doi.org/10.1509/jppm.25.2.160>. [Online]. Available: <https://doi.org/10.1509/jppm.25.2.160>.
- [21] K. Golladay and K. Holtfreter, 'The consequences of identity theft victimization: An examination of emotional and physical health outcomes', *Victims & Offenders*, vol. 12, no. 5, pp. 741–760, 2017. DOI: 10.1080/15564886.2016.1177766. eprint: <https://doi.org/10.1080/15564886.2016.1177766>. [Online]. Available: <https://doi.org/10.1080/15564886.2016.1177766>.
- [22] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer, 'Social phishing', eng, *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007, ISSN: 00010782.
- [23] B. Ur and Y. Wang, 'A cross-cultural framework for protecting user privacy in online social media', in *Proceedings of the 22Nd International Conference on World Wide Web*, ser. WWW '13 Companion, Rio de Janeiro, Brazil: ACM, 2013, pp. 755–762, ISBN: 978-1-4503-2038-2. DOI: 10.1145/2487788.2488037. [Online]. Available: <http://doi.acm.org/10.1145/2487788.2488037>.
- [24] J. M. Such and N. Criado, 'Multiparty privacy in social media', *Commun. ACM*, vol. 61, no. 8, pp. 74–81, Jul. 2018, ISSN: 0001-0782. DOI: 10.1145/3208039. [Online]. Available: <http://doi.acm.org/10.1145/3208039>.
- [25] A. Ivan, C. Iov, R. Lutai and M. Grad, 'Social media intelligence: Opportunities and limitations', eng, *CES Working Papers*, vol. 7, no. 2A, pp. 505–510, 2015, ISSN: 20677693. [Online]. Available: <http://search.proquest.com/docview/1718317015/>.
- [26] D. J. Solove, 'I've got nothing to hide and other misunderstandings of privacy', *San Diego L. Rev.*, vol. 44, p. 745, 2007.
- [27] D. Omand, J. Bartlett and C. Miller, 'Introducing social media intelligence (socmint)', eng, *Intelligence and National Security*, vol. 27, no. 6, pp. 801–823, 2012, ISSN: 0268-4527. [Online]. Available: <http://www.tandfonline.com/doi/abs/10.1080/02684527.2012.716965>.
- [28] C. V. Baccarella, T. F. Wagner, J. H. Kietzmann and I. P. McCarthy, 'Social media? it's serious! understanding the dark side of social media', *European Management Journal*, vol. 36, no. 4, pp. 431–438, 2018, ISSN: 0263-2373. DOI: <https://doi.org/10.1016/j.emj.2018.07.002>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0263237318300781>.

- [29] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda and C. Pu, 'Reverse social engineering attacks in online social networks', in *Detection of Intrusions and Malware, and Vulnerability Assessment*, T. Holz and H. Bos, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 55–74, ISBN: 978-3-642-22424-9.
- [30] M. Egele, G. Stringhini, C. Kruegel and G. Vigna, 'Towards detecting compromised accounts on social networks', eng, *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 4, pp. 447–460, 2017, ISSN: 1545-5971.
- [31] G. Warner-Søderholm, A. Bertsch, E. Sawe, D. Lee, T. Wolfe, J. Meyer, J. Engel and U. N. Fatilua, 'Who trusts social media?', *Computers in Human Behavior*, vol. 81, pp. 303–315, 2018, ISSN: 0747-5632. DOI: <https://doi.org/10.1016/j.chb.2017.12.026>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0747563217307021>.
- [32] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki *et al.*, 'Data breaches, phishing, or malware? understanding the risks of stolen credentials', in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 2017, pp. 1421–1434.
- [33] P. J. B. Nyblom, G. Wangen, M. Kianpour and G. Østby, 'The root causes of compromised accounts at the university', in *Proceedings of the 6th International Conference on Information Systems Security and Privacy*, SciTePress, 2020.
- [34] L. Gelinas, R. Pierce, S. Winkler, I. G. Cohen, H. F. Lynch and B. E. Bierer, 'Using social media as a research recruitment tool: Ethical issues and recommendations', *The American Journal of Bioethics*, vol. 17, no. 3, pp. 3–14, 2017.
- [35] V. Gkioulos, G. Wangen, S. K. Katsikas, G. Kavallieratos and P. Kotzanikolaou, 'Security awareness of the digital natives', *Information*, vol. 8, no. 2, p. 42, 2017.
- [36] G. Norman, 'Likert scales, levels of measurement and the "laws" of statistics', *Advances in health sciences education*, vol. 15, no. 5, pp. 625–632, 2010.
- [37] Wikipedia contributors, *Exif—Wikipedia, the free encyclopedia*, [Online; accessed 21-June-2020], 2020. [Online]. Available: <https://en.wikipedia.org/w/index.php?title=Exif&oldid=954241137>.
- [38] P. Grassi, M. Garcia and J. Fenton, *Nist special publication 800-63-3—digital identity guidelines*, 2017.

Appendix A

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
IT generally	329	1	4	3,12	0,863
Information security	329	1	4	3,26	0,735
Privacy	329	1	4	3,29	0,741
Valid N (listwise)	329				

Table A.1: Descriptives of the answers people gave about how they care about IT generally, information security and Privacy. where 1 is that they care very little and 4 that they care a lot.

	Have you ever gotten your social media account compromised?		
	Yes	No	Yes, but I have yet to receive my account back
	Count	Count	Count
More seldom	17	146	2
1-3 times a month	12	57	0
0-5 times a week	8	35	0
6- 10 times a week	6	11	1
11-15 times a week	0	1	0
16-20 times a week	1	2	0
More often than 20 times	0	12	0

Table A.2: Count of people how often people post on social media, looking at which people have gotten their accounts compromised

		Information security							
		1		2		3		4	
		Count	Percentage	Count	Percentage	Count	Percentage	Count	Percentage
Post image on FB	Very low	2	40,00%	14	37,80%	23	19,00%	13	12,70%
	Low	3	60,00%	19	51,40%	76	62,80%	62	60,80%
	High	0	0,00%	3	8,10%	20	16,50%	22	21,60%
	Very high	0	0,00%	1	2,70%	2	1,70%	5	4,90%
Posting about vacation FB	Very low	2	40,00%	4	10,80%	8	6,60%	4	3,90%
	Low	3	60,00%	25	67,60%	54	44,60%	40	39,20%
	High	0	0,00%	6	16,20%	43	35,50%	40	39,20%
Posting image of pets with name FB	Very high	0	0,00%	2	5,40%	16	13,20%	18	17,60%
	Very low	2	40,00%	18	48,60%	35	28,90%	32	31,40%
	Low	3	60,00%	17	45,90%	69	57,00%	48	47,10%
Post/share news FB	High	0	0,00%	2	5,40%	15	12,40%	15	14,70%
	Very high	0	0,00%	0	0,00%	2	1,70%	7	6,90%
	Very low	1	20,00%	20	54,10%	39	32,20%	26	25,50%
	Low	4	80,00%	15	40,50%	65	53,70%	54	52,90%
Post /share political FB	High	0	0,00%	2	5,40%	17	14,00%	17	16,70%
	Very high	0	0,00%	0	0,00%	0	0,00%	5	4,90%
	Very low	1	20,00%	8	21,60%	13	10,70%	8	7,80%
	Low	3	60,00%	15	40,50%	56	46,30%	44	43,10%
Post/share humorous FB	High	1	20,00%	11	29,70%	46	38,00%	35	34,30%
	Very high	0	0,00%	3	8,10%	6	5,00%	15	14,70%
	Very low	3	60,00%	16	43,20%	41	33,90%	25	24,50%
	Low	2	40,00%	17	45,90%	66	54,50%	64	62,70%
Participate in public debate FB	High	0	0,00%	4	10,80%	12	9,90%	8	7,80%
	Very high	0	0,00%	0	0,00%	2	1,70%	5	4,90%
	Very low	0	0,00%	7	18,90%	12	9,90%	5	4,90%
	Low	3	60,00%	13	35,10%	44	36,40%	37	36,30%
public debate FB	High	1	20,00%	14	37,80%	45	37,20%	37	36,30%
	Very high	1	20,00%	3	8,10%	20	16,50%	23	22,50%

Table A.3: Shows how people post on social media, in comparison to how much they said they cared about information security, where 1 caring little and 4 is caring a lot about information security.

		IT generally	Information security	Privacy
IT generally	Pearson Correlation	1	,528**	,299**
	Sig. (2-tailed)		0	0
	N	329	329	329
Information security	Pearson Correlation	,528**	1	,645**
	Sig. (2-tailed)	0		0
	N	329	329	329
Privacy	Pearson Correlation	,299**	,645**	1
	Sig. (2-tailed)	0	0	
	N	329	329	329
Post image on FB	Pearson Correlation	-,274**	0,05	0,092
	Sig. (2-tailed)	0,004	0,607	0,344
	N	107	107	107
Posting about vacation FB	Pearson Correlation	-0,001	,198*	0,155
	Sig. (2-tailed)	0,995	0,041	0,11
	N	107	107	107
Posting image of pets with name FB	Pearson Correlation	0,018	,245*	,193*
	Sig. (2-tailed)	0,858	0,011	0,046
	N	107	107	107
Post/share news FB	Pearson Correlation	-0,102	,221*	0,108
	Sig. (2-tailed)	0,298	0,022	0,266
	N	107	107	107
Post /share political FB	Pearson Correlation	0,021	,287**	0,143
	Sig. (2-tailed)	0,828	0,003	0,141
	N	107	107	107
Post/share humorous FB	Pearson Correlation	-0,108	,240*	0,144
	Sig. (2-tailed)	0,27	0,013	0,138
	N	107	107	107
Participate in public debate FB	Pearson Correlation	-0,007	,263**	0,148
	Sig. (2-tailed)	0,944	0,006	0,127
	N	107	107	107

Table A.4: Shows Person correlation between how much the respondents care about IT, information security, privacy and the perceived risk when performing different actions on Reddit.

		Privacy							
		1		2		3		4	
		Count	Percentage	Count	Percentage	Count	Percentage	Count	Percentage
Post image on Reddit	Very low	0	0,00%	5	45,50%	13	31,70%	20	36,40%
	Low	0	0,00%	5	45,50%	20	48,80%	21	38,20%
	High	0	0,00%	0	0,00%	7	17,10%	8	14,50%
	Very high	0	0,00%	1	9,10%	1	2,40%	6	10,90%
Posting about vacation Reddit	Very low	0	0,00%	5	45,50%	14	34,10%	20	36,40%
	Low	0	0,00%	5	45,50%	14	34,10%	12	21,80%
	High	0	0,00%	1	9,10%	9	22,00%	14	25,50%
	Very high	0	0,00%	0	0,00%	4	9,80%	9	16,40%
Posting image of pets with name Reddit	Very low	0	0,00%	7	63,60%	13	31,70%	15	27,30%
	Low	0	0,00%	2	18,20%	18	43,90%	23	41,80%
	High	0	0,00%	2	18,20%	8	19,50%	10	18,20%
	Very high	0	0,00%	0	0,00%	2	4,90%	7	12,70%
Post/share news Reddit	Very low	0	0,00%	8	72,70%	20	48,80%	29	52,70%
	Low	0	0,00%	2	18,20%	20	48,80%	20	36,40%
	High	0	0,00%	1	9,10%	1	2,40%	4	7,30%
	Very high	0	0,00%	0	0,00%	0	0,00%	2	3,60%
Post /share political Reddit	Very low	0	0,00%	7	63,60%	15	36,60%	20	36,40%
	Low	0	0,00%	2	18,20%	20	48,80%	20	36,40%
	High	0	0,00%	1	9,10%	6	14,60%	11	20,00%
	Very high	0	0,00%	1	9,10%	0	0,00%	4	7,30%
Post/share humorous Reddit	Very low	0	0,00%	8	72,70%	22	53,70%	29	52,70%
	Low	0	0,00%	3	27,30%	18	43,90%	22	40,00%
	High	0	0,00%	0	0,00%	1	2,40%	1	1,80%
	Very high	0	0,00%	0	0,00%	0	0,00%	3	5,50%
Participate in public debate Reddit	Very low	0	0,00%	7	63,60%	17	41,50%	24	43,60%
	Low	0	0,00%	3	27,30%	18	43,90%	18	32,70%
	High	0	0,00%	1	9,10%	6	14,60%	9	16,40%
	Very high	0	0,00%	0	0,00%	0	0,00%	4	7,30%

Table A.5: Shows how people post on Reddit, in comparison to how much they said they cared about privacy, where 1 caring little and 4 is caring a lot about privacy.

		Information security							
		1		2		3		4	
		Count	Percentage	Count	Percentage	Count	Percentage	Count	Percentage
Post image on Reddit	Very low	0	0,00%	8	50,00%	15	30,00%	15	37,50%
	Low	1	100,00%	5	31,30%	25	50,00%	15	37,50%
	High	0	0,00%	1	6,30%	8	16,00%	6	15,00%
	Very high	0	0,00%	2	12,50%	2	4,00%	4	10,00%
Posting about vacation Reddit	Very low	1	100,00%	8	50,00%	17	34,00%	13	32,50%
	Low	0	0,00%	6	37,50%	15	30,00%	10	25,00%
	High	0	0,00%	1	6,30%	13	26,00%	10	25,00%
	Very high	0	0,00%	1	6,30%	5	10,00%	7	17,50%
Posting image of pets with name Reddit	Very low	1	100,00%	10	62,50%	16	32,00%	8	20,00%
	Low	0	0,00%	3	18,80%	21	42,00%	19	47,50%
	High	0	0,00%	2	12,50%	10	20,00%	8	20,00%
	Very high	0	0,00%	1	6,30%	3	6,00%	5	12,50%
Post/share news Reddit	Very low	1	100,00%	12	75,00%	26	52,00%	18	45,00%
	Low	0	0,00%	4	25,00%	21	42,00%	17	42,50%
	High	0	0,00%	0	0,00%	2	4,00%	4	10,00%
	Very high	0	0,00%	0	0,00%	1	2,00%	1	2,50%
Post /share political Reddit	Very low	1	100,00%	11	68,80%	18	36,00%	12	30,00%
	Low	0	0,00%	4	25,00%	23	46,00%	15	37,50%
	High	0	0,00%	1	6,30%	7	14,00%	10	25,00%
	Very high	0	0,00%	0	0,00%	2	4,00%	3	7,50%
Post/share humorous Reddit	Very low	1	100,00%	13	81,30%	27	54,00%	18	45,00%
	Low	0	0,00%	3	18,80%	21	42,00%	19	47,50%
	High	0	0,00%	0	0,00%	1	2,00%	1	2,50%
	Very high	0	0,00%	0	0,00%	1	2,00%	2	5,00%
Participate in public debate Reddit	Very low	1	100,00%	11	68,80%	24	48,00%	12	30,00%
	Low	0	0,00%	3	18,80%	19	38,00%	17	42,50%
	High	0	0,00%	2	12,50%	5	10,00%	9	22,50%
	Very high	0	0,00%	0	0,00%	2	4,00%	2	5,00%

Table A.6: Shows how people post on Reddit, in comparison to how much they said they cared about Information security, where 1 caring little and 4 is caring a lot about information security.

		Participate in debate Reddit	Participate in debate Facebook	Participate in debate Twitter
Participate in debate Reddit	Pearson Correlation	1	,376**	,617**
	Sig. (2-tailed)		0,001	0
	N	107	75	38
Participate in debate Facebook	Pearson Correlation	,376**	1	,728**
	Sig. (2-tailed)	0,001		0
	N	75	265	110

Table A.7: Shows bivariate correlation analysis of what people chose to answer between the platforms on the question about debating on a platform

		Age			
		Younger than 30		31 and older	
		Count	Column N %	Count	Column N %
Genfer	Mann	139	70,60%	86	65,20%
	Woman	53	26,90%	46	34,80%
	Do not want to answer	5	2,50%	0	0,00%

Table A.8: Shows age and gender distribution for digital natives and non natives

ANOVA						
		Sum of Squares	df	Mean Square	F	Sig.
Full name	Between Groups	1,497	1	1,497	2,027	0,155
	Within Groups	237,122	321	0,739		
	Total	238,619	322			
Phone number	Between Groups	3,293	1	3,293	4,43	0,036
	Within Groups	238,614	321	0,743		
	Total	241,907	322			
Email	Between Groups	7,847	1	7,847	10,822	0,001
	Within Groups	232,044	320	0,725		
	Total	239,891	321			
Birth date	Between Groups	0,217	1	0,217	0,283	0,595
	Within Groups	246,41	322	0,765		
	Total	246,627	323			
Social security number	Between Groups	7,147	1	7,147	10,209	0,002
	Within Groups	224,723	321	0,7		
	Total	231,87	322			
Home address	Between Groups	2,911	1	2,911	4,012	0,046
	Within Groups	232,891	321	0,726		
	Total	235,802	322			
Account number	Between Groups	14,858	1	14,858	14,866	0
	Within Groups	319,816	320	0,999		
	Total	334,674	321			
Debit/credit card number	Between Groups	0,313	1	0,313	0,461	0,498
	Within Groups	218,083	321	0,679		
	Total	218,396	322			
Health data	Between Groups	0,634	1	0,634	0,675	0,412
	Within Groups	301,669	321	0,94		
	Total	302,303	322			

Table A.9: Shows an Anova that uses gender as factor and the perception on the usability of different data in use for ID-theft.

Descriptives									
		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
Full name	Younger than 30	224	2,32	0,859	0,057	2,2	2,43	1	4
	31 up	99	2,46	0,861	0,087	2,29	2,64	1	4
	Total	323	2,36	0,861	0,048	2,27	2,46	1	4
Phone number	Younger than 30	225	2,48	0,861	0,057	2,37	2,6	1	4
	31 up	98	2,7	0,864	0,087	2,53	2,88	1	4
	Total	323	2,55	0,867	0,048	2,46	2,65	1	4
Email	Younger than 30	223	2,44	0,857	0,057	2,33	2,55	1	4
	31 up	99	2,78	0,84	0,084	2,61	2,95	1	4
	Total	322	2,54	0,864	0,048	2,45	2,64	1	4
Birth date	Younger than 30	225	3,45	0,865	0,058	3,34	3,56	1	4
	31 up	99	3,51	0,896	0,09	3,33	3,68	1	4
	Total	324	3,47	0,874	0,049	3,37	3,56	1	4
Social security number	Younger than 30	224	2,5	0,831	0,056	2,39	2,6	1	4
	31 up	99	2,82	0,85	0,085	2,65	2,99	1	4
	Total	323	2,59	0,849	0,047	2,5	2,69	1	4
Home address	Younger than 30	224	2,49	0,847	0,057	2,38	2,6	1	4
	31 up	99	2,7	0,863	0,087	2,52	2,87	1	4
	Total	323	2,55	0,856	0,048	2,46	2,65	1	4
Account number	Younger than 30	224	3,05	1,049	0,07	2,92	3,19	1	4
	31 up	98	3,52	0,876	0,089	3,34	3,7	1	4
	Total	322	3,2	1,021	0,057	3,08	3,31	1	4
Debit/credit card number	Younger than 30	225	3,6	0,84	0,056	3,49	3,71	1	4
	31 up	98	3,66	0,786	0,079	3,51	3,82	1	4
	Total	323	3,62	0,824	0,046	3,53	3,71	1	4
Health data	Younger than 30	224	2,92	0,997	0,067	2,79	3,06	1	4
	31 up	99	3,02	0,903	0,091	2,84	3,2	1	4
	Total	323	2,95	0,969	0,054	2,85	3,06	1	4

Table A.10: Shows an Descriptives for gender and the perception on the usability of different data in use for ID-theft.

Descriptives									
		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
Full name	Younger than 30	196	2,35	0,836	0,06	2,23	2,46	1	4
	31 up	132	2,39	0,897	0,078	2,24	2,55	1	4
	Total	328	2,37	0,86	0,048	2,27	2,46	1	4
Phone number	Younger than 30	196	2,53	0,856	0,061	2,41	2,65	1	4
	31 up	132	2,61	0,889	0,077	2,45	2,76	1	4
	Total	328	2,56	0,869	0,048	2,47	2,66	1	4
Email	Younger than 30	195	2,55	0,88	0,063	2,42	2,67	1	4
	31 up	132	2,58	0,857	0,075	2,43	2,72	1	4
	Total	327	2,56	0,87	0,048	2,47	2,65	1	4
Birth date	Younger than 30	197	3,37	0,953	0,068	3,24	3,5	1	4
	31 up	132	3,6	0,74	0,064	3,47	3,73	1	4
	Total	329	3,46	0,88	0,048	3,37	3,56	1	4
Social security number	Younger than 30	196	2,48	0,819	0,059	2,37	2,6	1	4
	31 up	132	2,78	0,885	0,077	2,63	2,93	1	4
	Total	328	2,6	0,858	0,047	2,51	2,7	1	4
Home address	Younger than 30	197	2,55	0,853	0,061	2,43	2,67	1	4
	31 up	131	2,59	0,876	0,077	2,44	2,74	1	4
	Total	328	2,57	0,861	0,048	2,47	2,66	1	4
Account number	Younger than 30	196	3,11	1,074	0,077	2,96	3,26	1	4
	31 up	131	3,33	0,932	0,081	3,17	3,49	1	4
	Total	327	3,2	1,023	0,057	3,08	3,31	1	4
Debit/credit card number	Younger than 30	196	3,51	0,931	0,066	3,38	3,64	1	4
	31 up	132	3,77	0,6	0,052	3,67	3,88	1	4
	Total	328	3,62	0,823	0,045	3,53	3,71	1	4
Health data	Younger than 30	197	2,91	0,975	0,069	2,77	3,05	1	4
	31 up	131	3,03	0,96	0,084	2,86	3,2	1	4
	Total	328	2,96	0,97	0,054	2,85	3,06	1	4

Table A.11: Shows descriptives for digital natives and non-natives to what degree they believe that information can be used in performing identity theft

		Have you ever had your account on social media hacked?					
		Yes		No		Yes, but I have yet to regain access to my account	
		Count	Percentage	Count	Percentage	Count	Percentage
Age	Younger than 30	31	15,70%	165	83,80%	1	0,50%
	31 and above	16	12,10%	114	86,40%	2	1,50%
Gender	Mann	25	11,10%	199	88,40%	1	0,40%
	Woman	22	22,20%	75	75,80%	2	2,00%
	Prefer not to answer	0	0,00%	5	100,00%	0	0,00%
Municipality	Agder	0	0,00%	6	100,00%	0	0,00%
	Innlandet	10	17,50%	47	82,50%	0	0,00%
	Møre og Romsdal	3	37,50%	5	62,50%	0	0,00%
	Nordland	1	12,50%	7	87,50%	0	0,00%
	Oslo	13	16,50%	66	83,50%	0	0,00%
	Vestfold og Telemark	3	20,00%	12	80,00%	0	0,00%
	Troms of Finnmark	1	9,10%	10	90,90%	0	0,00%
	Trøndelag	2	5,70%	33	94,30%	0	0,00%
	Vestland	2	7,40%	25	92,60%	0	0,00%
	Viken	2	4,00%	47	94,00%	1	2,00%
Highest reched education	Rogaland	0	0,00%	9	100,00%	0	0,00%
	Ingen	0	0,00%	1	100,00%	0	0,00%
	Primary school	0	0,00%	7	100,00%	0	0,00%
	High school	10	18,20%	45	81,80%	0	0,00%
	Vocation school	1	11,10%	7	77,80%	1	11,10%
	University and college, up to and including 4 years	17	12,00%	125	88,00%	0	0,00%
	University and college, longer than 4 years	9	10,20%	79	89,80%	0	0,00%
On a scale from 1-4 IT skill	Unspecified or no complete education	0	0,00%	3	100,00%	0	0,00%
	1	0	0,00%	1	100,00%	0	0,00%
	2	15	25,90%	42	72,40%	1	1,70%
	3	21	15,70%	111	82,80%	2	1,50%
	4	11	8,10%	125	91,90%	0	0,00%

Table A.12: Shows what demographic groups that have experienced having their accounts compromised.

Appendix B

Questionnaire

Risikoppfatning sosiale medier - Reddit

Side 1

Denne spørreundersøkelsen er laget i forbindelse med masteroppgaven min ved NTNU ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi. Oppgaven dreier seg om risikoppfatning på sosiale medier, og ID-tyveri, og er designet for å få en større forståelse rundt denne tematikken. Spørreundersøkelsen vil ta ca. 10 minutter å gjennomføre.

Det er kun jeg og veilederen min på masteroppgaven som vil kunne se på innsamlet data. Jeg setter veldig pris på alle som velger å svare på spørreundersøkelsen. All informasjon samles inn anonymt, og dataen vil kun bli brukt i forbindelse med dette studiet.

Hvis du har spørsmål til studien kan du ta kontakt kontakt til:

- Philip Nyblom, philipny@stud.ntnu.no eller veileder Gaute Wangen, gaute.wangen@ntnu.no

-Philip Nyblom

Jeg har mottatt og forstått informasjon om prosjektet Risikoppfatning sosiale medier, og har fått anledning til å stille spørsmål.

Ved å trykke "Neste side" samtykker jeg til at mine opplysninger blir behandlet frem til prosjektet er avsluttet.



Side 2

Alder? *

Kjønn? *

Fylke? *

Hva er ditt høyeste fullførte utdanningsnivå? *

På en skala fra 1-4 hvor IT kyndig er du?

Hvor 1 er svært lite kyndig og 4 er veldig kyndig.

1 2 3 4

På en skala fra 1-4 hvor mye bryr du deg om...

1 Bryr meg svært lite


4 Bryr meg veldig

	1	2	3	4
IT generelt *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Informasjonssikkerhet *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Personvern *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Hvilke sosiale medier benytter du deg av? *

- Facebook
- Instagram
- Twitter
- Reddit
- TikTok
- Snapchat
- Andre

Hvilke andre sosiale medier benytter du deg av?

-  Dette elementet vises kun dersom alternativet «Andre» er valgt i spørsmålet «Hvilke sosiale medier benytter du deg av?»

Hvor ofte legger du ut innlegg på sosiale medier i en gjennomsnittlig uke?

- Sjeldnere
- 1-3 ganger i måneden

- 0-5 ganger i uken
- 6- 10 ganger i uken
- 11-15 ganger i uken
- 16-20 ganger i uken
- Oftere enn 20 ganger

Hvor ofte oppdaterer du de forskjellige enhetene du bruker til å surfe på sosiale medier?

Oppdatering i form av oppdateringene programmer spør om.

	Hver måned	Annenhver måned	Sjeldnere enn annenhver måned	Har ikke enheten/bruker den ikke til sosiale medier	Vet ikke	Når programmet ber om det	Har ikke enheten
Mobil (android/mac)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PC/Mac	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Nettbrett	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

 Sideskift

Side 3

Scenario

Her kommer et scenario, svar slik du tror du ville reagert.




Du får en melding, i denne meldingen ligger det med en lenke, trykker du på denne?
Meldingen kommer fra...

Du kan se et eksempel på en slik melding i bildet ovenfor.

	Ja	Nei	Kanskje
En bekjent *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
En venn *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Familie *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Nær familie *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

 Sideskift

Side 4

 Dette elementet vises kun dersom alternativet «Facebook» er valgt i spørsmålet «Hvilke sosiale medier benytter du deg av?»

Hvordan oppfatter du risiko når du utfører følgende handlinger på Facebook/Instagram?

Med risiko mener vi muligheten og konsekvensen for at noe negativt kommer til å skje som følge av en handling.

	Svært lav	Lav	Høy	Veldig høy
	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Legger ut bilder *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legger ut om at du er på ferie *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legger ut bilder av husdyr med navn *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/legger ut en nyhetssak *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/Legger ut noe politisk *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/Legger ut noe med humoristisk innhold *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deltar i offentlig debatt på plattformen *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

i Dette elementet vises kun dersom alternativet «Twitter» er valgt i spørsmålet «Hvilke sosiale medier benytter du deg av?»

Hvordan oppfatter du risiko når du utfører følgende handlinger på Twitter?

Med risiko mener vi muligheten og konsekvensen for at noe negativt kommer til å skje som følge av en handling.

	Svært lav	Lav	Høy	Veldig høy
Legger ut bilder *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legger ut om at du er på ferie *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legger ut bilder av husdyr med navn *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/legger ut en nyhetssak *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/Legger ut noe politisk *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/Legger ut noe humoristisk innhold *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Deltar i offentlig debatt på plattformen *

Hvordan oppfatter du risiko når du utfører følgende handlinger på Reddit?

Med risiko mener vi muligheten og konsekvensen for at noe negativt kommer til å skje som følge av en handling.

	Svært lav	Lav	Høy	Veldig høy
Legger ut bilder *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legger ut om at du er på ferie *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legger ut bilder av husdyr med navn *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/legger ut en nyhetssak *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/Legger ut noe politisk *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/Legger ut noe humoristisk innhold *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deltar i offentlig debatt på plattformen *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Dette elementet vises kun dersom alternativet «Snapchat» er valgt i spørsmålet «Hvilke sosiale medier benytter du deg av?»

Hvordan oppfatter du risiko når du utfører følgende handlinger på Snapchat?

Med risiko mener vi muligheten og konsekvensen for at noe negativt kommer til å skje som følge av en handling.

	Svært lav	Lav	Høy	Veldig høy
Legger ut bilder *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legger ut om at du er på ferie *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Legger ut bilder av husdyr med navn *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Deler/Legger ut noe humoristisk innhold *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Benytter deg av Snapmap *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bruker du samme passord på sosiale medier som på andre sider? *

- Jeg bruker alltid samme passord til alt
- Jeg bruker samme passord på alt, men tofaktoraутентisering der det er mulig
- Jeg bruker små variasjoner av det samme passordet på forskjellige steder
- Jeg bruker alltid forskjellige passord
- Jeg bruker forskjellige passord, og tofaktoraутентisering på alt der det er mulig

Har du endret på personvernsinnstillinger for å gjøre profilen din mindre synlig? *

Jeg begrenser så godt som mulig...

På en skala fra 1-4 hvor 1 er veldig lite og 4 er veldig mye.

Alle disse utsagnene gjelder sosiale medier.

	1	2	3	4	Vet ikke
hvem som kan se profilen min på sosiale medier *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
hvem som kan se kontaktinformasjonen min *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
hvem som kan se innleggene mine *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
hvem som kan se vennelisten/følgere mine *	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

søkemotorer sin mulighet til å vise profilene mine *

Hvilken informasjon har du offentlig synlig på profilen din? *

- E-post adresse
- Hjemby
- Telefonnummer
- Bilder av deg med familie
- Politisk ståsted
- Forhold
- Familiemedlemmer
- Legning
- Har ikke oversikt
- Har skjult alt som lar seg skjule

 Sideskift

Side 5

I hvilken grad tror du denne informasjonen kan bli missbrukt, til å utføre et ID-tyveri mot deg?

ID-tyveri kan enten være at noen overtar en av kontoene dine eller at man bruker informasjonen din for å svindle deg.

	Svært lite	Lite	Mye	Svært mye
Fullt navn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Telefonnummer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
E-post	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fødselsnummer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Fødselsdato	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hjemmeadresse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kontonummer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bankkort/kredittkort nummer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Helsedata	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kontoinformasjon og passord	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>




Side 6

Har du noen gang fått din konto på sosiale medier hacket? *

- Ja
- Nei
- Ja, men har ikke fått kontoen tilbake enda

Vet du hvordan kontoen din ble hacket? *

-  Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du noen gang fått din konto på sosiale medier hacket?»
- Phishing
- Delte passordet til en jeg har relasjon med
- Hacket
- Annet
- Nei/vet ikke

Hvordan ble du hacket? *

- i** Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Vet du hvordan kontoen din ble hacket?»

Hva har konsekvensene vært, hva har kontoen blitt brukt til? *

- i** Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du noen gang fått din konto på sosiale medier hacket?»

Hvilke tiltak har du tatt for å sikre kontoene dine på sosiale medier? *

- i** Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du noen gang fått din konto på sosiale medier hacket?»

- Satt på totrinnsbekreftelse
- Byttet passord til et som er kortere enn 12 tegn
- Byttet passord til et som er 12 tegn eller lengere
- Startet å bytte passord regelmessig
- Fått det sosiale mediet om å varsle hver gang du logger deg på fra en ny enhet/nytt geografisk område
- Benytter anti-virus
- Har maskinen sin brannmur skrudd på
- Andre

Hvor ofte bytter du passord? *

i Dette elementet vises kun dersom alternativet «Startet å bytte passord regelmessig» er valgt i spørsmålet «Hvilke tiltak har du tatt for å sikre kontoene dine på sosiale medier?»

- oftere enn hver måned
- Hver måned
- Hver tredje måned
- Hvert halvår
- Hvert år
- Sjeldnere enn hvert år

Hvilke andre tiltak har du brukt? *

i Dette elementet vises kun dersom alternativet «Andre» er valgt i spørsmålet «Hvilke tiltak har du tatt for å sikre kontoene dine på sosiale medier?»

Har du blitt hacket igjen etter å ha implementert tiltak? *

i Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du noen gang fått din konto på sosiale medier hacket?»

- Ja
- Nei
- Har ikke implementert noen tiltak

Har du noen formening om hvorfor de tiltakene ikke har fungert/vært tilstrekkelig nok? *

i Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du blitt hacket igjen etter å ha implementert tiltak?»

Selv om du ikke har fått kontoen tilbake enda, vet du hvordan kontoen din ble hacket? *

i Dette elementet vises kun dersom alternativet «Ja, men har ikke fått kontoen tilbake enda» er valgt i spørsmålet «Har du noen gang fått din konto på sosiale medier hacket?»

- Phishing
- Delte passordet til en jeg har relasjon med
- Hacket
- Annet
- Nei/vet ikke

Hvordan ble du hacket? *

i Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Selv om du ikke har fått kontoen tilbake enda, vet du hvordan kontoen din ble hacket?»

Vet du hva kontoen blir/har blitt brukt til? *

i Dette elementet vises kun dersom alternativet «Ja, men har ikke fått kontoen tilbake enda» er valgt i spørsmålet «Har du noen gang fått din konto på sosiale medier hacket?»

**Hva tror du kontoen din på sosiale medier kan bli brukt til om den blir hacket? ***



Dette elementet vises kun dersom alternativet «Nei» er valgt i spørsmålet «Har du noen gang fått din konto på sosiale medier hacket?»

Tilbakemelding om spørreundersøkelsen.

Her kan du skrive tilbakemelding på spørreundersøkelsen.

Se nylige endringer i Nettskjema (v1023_0)

