future internet

MDPI

Article

Risk Perceptions on Social Media Use in Norway

Philip Nyblom [1,*,†], Gaute Wangen [2,*,†] and Vasileios Gkioulos [1,*]

[1] Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU–Norwegian University of Science and Technology, 2815 Gjøvik, Norway
[2] IT Division, Digital Security Section, NTNU–Norwegian University of Science and Technology, 2815 Gjøvik, Norway
* Correspondence: philip.nyblom@gmail.com (P.N.); gaute.wangen@ntnu.no (G.W.); vasileios.gkioulos@ntnu.no (V.G.)
† These authors contributed equally to this work.

Received: 15 October 2020; Accepted: 23 November 2020; Published: 26 November 2020

Abstract: Social media are getting more and more ingrained into everybody's lives. With people's more substantial presence on social media, threat actors exploit the platforms and the information that people share there to deploy and execute various types of attacks. This paper focuses on the Norwegian population, exploring how people perceive risks arising from the use of social media, focusing on the analysis of specific indicators such as age, sexes and differences among the users of distinct social media platforms. For data collection, a questionnaire was structured and deployed towards the users of multiple social media platforms (total n = 329). The analysis compares risk perceptions of using the social media platforms Facebook (n = 288), Twitter (n = 134), Reddit (n = 189) and Snapchat (n = 267). Furthermore, the paper analyses the differences between the sexes and between the digital natives and non-natives. Our sample also includes sufferers of ID theft (n = 50). We analyse how account compromise occurs and how suffering ID theft changes behaviour and perception. The results show significant discrepancies in the risk perception among the social media platform users across the examined indicators, but also explicit variations on how this affects the associated usage patterns. Based on the results, we propose a generic risk ranking of social media platforms, activities, sharing and a threat model for SoMe users. The results show the lack of a unified perception of risk on social media, indicating the need for targeted security awareness enhancement mechanisms focusing on this topic.

Keywords: digital natives; identity theft; risk; risk perception; security; security awareness; social media; user behaviour

1. Introduction

Identity theft and account hacking are significant security threats in the digital era. Today's societies are deeply interconnected and reliant on digitally offered services with most of the peoples' everyday dealings, including banking and their payments, happening online and via mobile devices. *Have I been pwned* (https://haveibeenpwned.com/ Visited Oct 2020) is an online database comprising leaked credentials for accounts claiming to consist of over 10 billion usernames and passwords.

The consequences and effect propagation of identity theft are further intensified when considering the potential for social engineering through social media (SoMe) misuse. In the past, a multitude of hacked SoMe accounts have been exploited to disseminate lies, spearhead phishing campaigns, request and process illegitimate payments and even influence the stock markets. A well-known case of a high profile SoMe account that was hacked could be Skype's Twitter account back in 2014 (https://www.theverge.com/2014/1/1/5264540/skype-twitter-facebook-blog-accounts-hacked), that was employed by the attackers to post a tweet with the text "Do not use Microsoft emails...".

Given the plethora of relevant attack vectors and the probable direct impact on the general population, it is essential to establish suitable awareness campaigns to enhance the security posture of the society and lessen the impact of such attacks, as discussed by Al-Charchafchi et al. [1] who reviewed threats against information privacy and security in social networks. The initial step in this direction is to analyse how people perceive the risk they are exposed to when using SoMe and assess the impact of specific indicators (such as age and sex) when evaluating such risks. Such an analysis must be undertaken taking into account the national or regional context, such as ICT (Information and Communication Technologies) penetration, digital preparedness and acceptance metrics, avoiding unfounded generalisations across borders or groups. Thus, national and regional studies can offer a suitable mapping of the current societal security posture, preparedness and resilience, as well as suitable metrics to establish enhancement methods.

Accordingly, in this study we focus on the Norwegian population, measuring public risk perception on the use of SoMe, reviewing what people freely post and how an attacker can exploit this content, also focusing on how being a victim of identity theft affects a posteriori risk perception and usage patterns. This study was motivated by the fact that the Norwegian society is highly digitised, steadily achieving growing Digital Economy and Society Index (DESI) scores for the past years while consistently being evaluated above the EU average, with a 2020 score of 69.5 against an EU average of 52.6.

SoMe are extensively utilised while being an open platform where people tend to over-share. This over-sharing might cause break-ins, a stolen identity, stalking and more, physical or virtual consequences. For example, houses being targeted while people are on holiday or accounts being hijacked by an attacker using social engineering. The security risk might not be the primary thought of people when posting information online, even though they might volunteer more information than one might think is prudent, had they shared the same information in real life/in person.

The Norwegian data authority defines identity theft as: *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*, while the Norwegian punitive law §202 stipulates:

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 obtain an unjustified gain for himself or another, or inflict another loss or disadvantage.

Additionally, this paper examines variations in risk perceptions between digital natives and non-natives, where digital natives are defined as people born after 1987 [2]. The contributions of this article are:

1. Investigate the following areas in sharing habits and exploitation for ID theft on SoMe in Norway.
    (a) Are there differences in security routines between Digital natives and non-natives?
    (b) Are there differences in security routines between genders?
    (c) Does having suffered ID or account theft change security routines?
2. Investigate how people perceive the risk of ID theft on SoMe.
    (a) Differences in risk perceptions across popular SoMe platforms (Facebook, Twitter, Reddit and Snapchat)
    (b) Are there differences in risk perceptions between digital natives and non-natives?
    (c) Are there differences in risk perceptions between genders?
    (d) Does having suffered ID or account theft change risk perceptions on sharing habits?
3. How does ID theft occur and what are the consequences?

As detailed in the research questions above, the included SoMe platforms are Facebook, Twitter, Reddit and Snapchat. A brief description of these services is a follows (worldwide user estimates

were collected from Oberlo.com for October 2020): Facebook is a social media platform that offers the opportunity to mostly vet who may see things about you and who can see your posts. Some information are not private by default, like friends list and information about the account holder. Facebook has 2.7 billion users. Twitter is a micro-blogging service where everything that is posted there is public by default. How one connects on Twitter is by actively choosing to follow different people. Compared to Facebook, where both parties have to actively accept becoming friends, one can follow whoever they want on Twitter without them having to say yes or no. The platform has a character count maximum of 240 characters, to keep the posts (tweets) short. Twitter is estimated to have 340 million users worldwide. Reddit is a social media that is more anonymous by nature, while very few subscribers use their name on their Reddit profiles. Reddit is partitioned into different subreddits where people can come together as various parties interested in the same thing; for example, there are subreddits for cats, politics and games. With how Reddit is structured there is a risk for Echo chambers to be formed, where people of the same thought keep agreeing to each other. Reddit is estimated to have 430 million users. Finally, Snapchat is a picture sharing service, where images one sends also get deleted after a set amount of time, and after the recipient has viewed an image, it gets deleted. If the recipient takes a screenshot of the image that they receive, the sender of the message receives a notification. Snapchat is estimated to have 230 million users worldwide.

A recent study by Studen [3] investigated social media as a cultural and economic phenomenon, exploring their expected future developments through an international two-stage Delphi study. The study indicates that enhanced interaction on platforms, as well as platform diversification is expected, promoting social media as the predominant news distributor, also increasing their societal and psychological impact. Our principal contribution is knowledge regarding the risk perceptions concerning ID theft using SoMe platforms, and how users perceive the risk of conducting certain activities on the surveyed platforms. Our paper outlines which information assets the participants deem worthy of protection and what they fear on SoMe. Our paper proposes a novel threat model for SoMe users derived from the results. Finally, we go in depth into how ID theft occurs, and the suffered and perceived consequences of suffering a security breach.

We have structured the remainder of this article as follows: The following section presents related work focusing among others on the areas of risk perception, ID theft and social media. Section 2 presents the methods used for this study discussing the instrument and the processes used for recruitment, data collection and analysis. Section 3 presents the sample demographics and discusses the representativity of the sample. Furthermore, Section 4 contains the complete analysis of the results, separating them into three major categories, firstly referring to routines, then risk perception and finally, risk perception alterations after suffering identity theft. Section 5 summarises the results and discusses the research questions. Lastly, we present the conclusions, which provide key takeaways and close the paper. The conclusions also include research limitations, impacts and recommendations for future research.

2. Related Work

There are multiple studies on risk perception, compromised accounts and SoMe, in this section we will explore some of these works to give the reader a better impression of the foundations for the development of this paper.

Several studies focus on the foundations of risk perception measurement: Slovic, Fischhoff and Lichtenstein [4] explored risk perception and explained that people, when asked about the risk of something, rarely 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 risk. These heuristics create misalignments between the actual risk and the perceived risk, that experts should try to close when discussing risk with a layperson. Additionally, Alhakami and Slovic [5] explore how risk and benefit relate to each other. They observed that if the perceived risks were high, the perceived benefits would be perceived as low, and something that is perceived to have high benefit is commonly perceived to

have low risk. The authors asked psychology students to rate how risky something was towards the US. The students could 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. Furthermore, Slovic et al. [6] examined how experience changes how we perceive risk, and how heuristics change 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. [7]; one is the rationale system, meaning 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 when an event happens. Loewenstein mentions that researchers should take into account such an emotional reaction to risks. Worth mentioning are the findings by Gustafsod [8], who wrote a paper about how men and women perceive risk differently. The findings document the existing around gender differences and risk perception. Most papers he saw that tackled risk perception had a quantitative method where you ended up with females having a higher perceived risk. He talks a bit about how the power relations between males and females on how women often fear crime and that this stems from fear of male sexual violence.

Other ground breaking work within the measurement of risk perception focus on the "Risk compensation model" by Adams [9]; the "presentation of risk information" and the "Availability of risk information" discussed by Kahneman [10]; the psychometric based "Expressed risk preferences" and the "Affect in risk perception" [11] which evaluates the affect of heuristic in judgments of risks and benefits.

Accordingly, it becomes clear that a variety of theoretical and empirically supported approaches have been developed in order to support the understanding of how risk perceptions may be shaped, as discussed by Paul van Schaik [12], whose study motivates further efforts into identifying the determinants of people's behaviour towards cyber risk on the Internet. Furthermore, Yixin Zou [13] conducted a survey investigating the acceptance of commonly recommended online safety practices (on security, privacy and identity theft protection), establishing both discrepancies and the respective reasons for non-compliance.

Another aspect that may influence risk perception is security awareness. Focusing on rural Norway, an earlier stydy by Gunleifsen et al. [14] researched security awareness, perceptions and the culture of participants from rural Norway. They collected the sample from a broadband subscriber list and had n = 945 with 76% males and an average age of 56 years. The authors surveyed attitude toward IT, knowledge, risk evaluations, trust in authorities, training preferences and compare risk-evaluations with their online behaviour. The results show that the level of security awareness is highly subjective and that training programs and security awareness campaigns are both needed and requested by end-users. The risk perception part of Gunleifsen et al. measures confidence in the ability to judge what is safe or not in cyberspace, and how much the participants worry about certain abuse scenarios.

Additionally, like the study presented in this article, what happens to people after having been victims of identity theft is explored in the paper by Golladay and Holtfreter [15] where they explore the health detriments, and the emotional harms that being a victim of identity theft, can cause. They found that, for example, age impacts the emotional response of a victim where older people get affected more than younger people. In a broader scope, a report by Newman [16] discusses various aspects of ID theft, including its various types, victims demographics and the typology of the offenders, also including an analysis regarding the various costs of ID theft at the financial, personal and societal levels. This report, that has been funded by the U.S. Department of Justice, explicitly recommends future research on routine activities and decisions that lead to the victimisation of individuals, in order to identify vulnerable populations and identify behavioural patterns that may lead to effective interventions.

Additionally, a wide variety of studies has explored specific aspects of ID theft, focusing on specific target groups, application domains and technologies, or sectors.

Jagatic et al. wrote a paper [17] where they tried to see if knowing the person who sends a phishing link affects 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 they provided the phishing link 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. Milne, Rohm and Bahl [18] looks at how consumers protect their personal information on the internet regarding the threat of identity theft and seeing if there are any predictors for the level of online protection is practiced. 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 Centre for Democracy and Technology (2003). This paper was inspiring to look at for how they researched identity theft. One question they asked were if people "Refused to give information to a website because you felt it was too personal."

Furthermore, Thomas et al. [19] 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. Finally, Nyblom et al. [20] used a root cause method 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%. As discussed earlier, these studies, although they may appear fragmented, are targeted by design to specific target groups, indicators or technologies, narrowing the scope and allowing the construction of a more complete and detailed picture regarding the determinants of human behaviour towards cyber risk.

Ur and Wang [21] 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 layer 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).

Focusing on social media, the paper by Such and Cirado [22] 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 coping strategies for how one can and should share information on social media, and what the major drawbacks these coping strategies might have. It also proposes some different strategies that can be used when posting multi-party privacy-related posts. A similar study to this one was conducted by Schaik et al. [23], which measured risk perceptions of security and privacy in online social networking. The study applied psychometric methods to survey 201 Facebook users from the UK. Their primary findings was that the concern was highest for information-sharing related to privacy. An additional aspect that has been examined in the literature is specific strategies to protect the privacy of users, and potential impact of integrating privacy policies on the information-sharing behaviour of the users. Damion et al. investigated this aspect [24], by analysing 51 papers on SoMe privacy, concluding that despite the user concern on ID theft and third party access to their information, integrated privacy policies do not directly affect the users information sharing behaviour. A variety of studies focus on the security implication of social media as platforms and also specifically their use, such as the study by Wu [25] who reviewed social media security risks and existing mitigation techniques, and the book by Gonzales [26] that draws a much broader picture on online activity, including aspects related with the collection, storage and use of data, the management of intellectual property and online activism.

Looking at what are the best practices for people to protect their social media account, we looked at a public advisory company called NorSIS and Nettvett which are governmental owned companies in Norway, that strive for cybersecurity awareness for the public and small/medium enterprises.

Of their recommendations for how one can reduce the risk on ID theft when using the internet, one of their recommendations is for people to not give away personal information to unknown people on the internet, without the person giving away information being the one who instigates the information transfer (https://nettvett.no/forebygge-identitetsverdi/). Nettvett also has some preventative measures for people who are exposed to blackmail on social media, in their list they suggest hiding friends lists, hiding the profile from search engines and making sure that the profiles timeline is just visible to friends (https://slettmeg.no/seksuell-utpressing-pa-nett/).

There has been a lot of original works done on risk, risk perception and risk awareness that this study builds on. We usually define risk as the consequence and probability of something happening, but this definition might be a bit too narrow for when measuring risk in laypeople. As Slovic mentioned [27], the heuristics of a person has an impact in how they perceive and rate risk. Bickerstaff K. [28] mentioned that most risk perception studies at the time had been conducted mostly in with questionnaires, but that more recently more studies had used or supplemented their quantitative data with qualitative data. There does not seem to be many papers written about the risk perception of people in social media and especially how people perceive the risk of a compromised social media account. We want to contribute in filling this gap, 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.

This study builds upon our earlier results at [29] which focused on evaluating the conceptual models used by security experts when developing security solutions targeted towards the general public, [2] which focused on analysing the security awareness divergences of digital natives across Norway and two other European countries, [14] that focused on evaluating the security awareness within the rural Norwegian population, and [20] which focused on identifying the root cause of compromised accounts at Norwegian university. These studies are complementary to each other, and to other national reports [30], aiming to solidify a more clear understanding on the cyber security culture of the Norwegian society.

Furthermore, the literature study has revealed two aspects of risk perceptions that have not been addressed: Several studies measure risk perceptions on one SoMe platform [12,23], but they have made no comparisons of risk perceptions between services. Additionally, while ID theft and account compromise have received some attention [17–20], we did not find any studies on how suffering ID theft changes risk perceptions.

The results of these initiatives are of National interest, since they provide a more clear understanding regarding the current status of cybersecurity awareness, thus allowing for enhancements on the content (e.g., general, introductory, comprehensive), format (e.g., promotional, informational, enforcing) and delivery types of enhancement programs. Furthermore, the results are also of a wider interest, as Norway is one of the most highly digitised counties in the world, with significant penetration of information and communication technologies, while still operating within the wider European context. Thus, providing future perspectives, as digitization progresses across the continent.

3. Method

In this chapter, we will describe the applied research strategies. There are many ways one can go about researching risk perception and risk awareness of people. This study aimed to gather data about the risk perception of ID theft in the Norwegian population and therefore needed a broader sample. Additionally, one of the research questions aimed to gather data from people who had suffered ID theft.

The data collection went from May to June 2020.

3.1. Instrument

As seen in the related work section, one of the most common approaches to measure the risk perception of people is using a questionnaire [5]. Questionnaires allow us to reach out to and sample a broader part of the population. The questionnaire used for this project builds on previous work on how to measure people's risk perception and followed Milne, Rohm and Bahl [18]. It contained questions based on the current best practice advice from a trusted authority on how not to get one's identity stolen. Additionally, we followed NorSIS advice and guidelines on how to prevent identity theft. (NorSIS is an independent organisation and partner to the government, businesses and research facilities in the subject of cybersecurity. https://nettvett.no/forebygge-identitetsverdi/) Quality assurance was done through multiple testing rounds with representatives from the sample demographic to ensure appropriate wording and measurements.

The questionnaire totalled 30 primary questions, a summary of the questionnaire with surveyed topics, number of questions, target group and objectives is seen in Table 1, and the whole instrument is available in Appendix A. The survey started with four demographic, two self-assessment and three questions to establish the respondent's social media presence. These initial questions were all mandatory. Furthermore, the remaining questions asked the respondent about various security routines, risk perceptions and ID theft. We designed the questions regarding security routines to gauge the respondent's susceptibility to ID theft. We designed seven questions as matrices with rating scales for multiple variables, e.g., question 6: *How much do you care about [...] (1) IT in general, (2) Information security, (3) Privacy*. These were designed with ordinal scales.

Table 1. Summary of the questionnaire: No of questions per topic, target group and measurement objective per question group.

Q nr	Topic	No. of Questions	Target Group	Measurement Objective
1–4	Demography	4	All	Sample tendencies, categories and biases
5–6	Self-assessment	2	All	Perceived competence and interest in security related topics
7–9	Social media presence	3	All	Measure social media presence and activity for determining later questions
10	Security routine	1	All	Measure update practices for owned devices (Smartphone, PC/Mac, Tablet)
11	Scenario assessment	1	All	Risk perception and trust in social circles
12	Risk perception	1	Facebook users	Risk perception when conducting different activities on Facebook
13	Risk perception	1	Twitter users	Risk perception when conducting different activities on Twitter
14	Risk perception	1	Reddit users	Risk perception when conducting different activities on Reddit
15	Risk perception	1	Snapchat users	Risk perception when conducting different activities on Snapchat
16	Security routine	1	All	Password security
17–19	Security routine	3	All	Risk exposure through security and privacy settings on social media accounts.
20	Risk perception	1	All	Risk perception on abuse of shared information.
21	ID theft	1	All	Determine of the respondent ever had his/hers account hacked
22–28	ID theft	6	Hacked	Determine how the ID theft occurred, suffered consequences, post-incident security routines.
29	ID theft	1	Not hacked	Awareness of and thoughts on ID abuse
30	Quality assurance	1	All	Feedback on the questionnaire

The design of the survey was such that some answers triggered specific follow-up questions. The most significant break-off point in the questionnaire was when the respondents were asked whether they ever had their accounts hacked. If the answer was "Yes" (*Hacked* group), they were asked seven additional questions specifically about the ID theft incident, see question 21 in Table 1. If the respondents answered no (*not hacked*), they were asked one question regarding ID theft (Q29).

3.2. Recruitment and Data Collection

The recruitment strategy aimed at recruiting both from the general population together with people that had suffered from ID theft. We limited the sample population to only include Norwegians, and the online questionnaire was only available in the Norwegian language. For sample control, we conducted the sampling with three copies of the questionnaire distributed on three different platforms. To recruit from the sample population that had suffered ID theft, we were allowed to distribute the questionnaire through Slettmeg.no, which is a service for helping people that have suffered ID theft and other cyber incidents. To obtain a sample from the generic population, we distributed a second questionnaire through Facebook and Twitter, and the third on the Norwegian Reddit forums. Furthermore, we attempted to recruit the respondents from Slettmeg.no who had suffered ID theft for in-depth interviews. However, from the limited pool of compromised accounts, only two people answered the further inquiry.

3.3. Data Analysis

The compared groups in this study are the sexes (male/female), age and hacked groups. We have also split the collected ages into digital natives and non-digital natives; as there might be a difference in how the digital natives perceive risk on social media. Gkioulos et al. [29] defined digital natives as people born between 1987 and 1997. We classified participants younger than 31 as digital natives, and those above as non-natives, to comply with this definition as much as possible for the available sample. When analysing differences between the sexes, we left the group that had chosen ''prefer not to answer" out because of the low number of respondents that chose this option, with only five people being in the group. We sorted the hacked/not hacked group using question 21 in the survey.

To process the results of the questionnaire, we applied a variety of statistical data analysis methods available through the IBM SPSS software v2.0. A summary of the statistical tests used in this research is as follows:

Firstly, each variable was analysed separately, looking at trends and distribution with histograms and descriptives. Furthermore, we performed bivariate analysis and ANOVA on age, gender and hacked groups to investigate differences. We treated "No" as zero and "Yes" as one in the analysis for binary-type questions. We 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. A thing to note is that the use of ANOVA or other bivariate methods for analysing ordinal nonlinear data has been criticised for not being normally distributed. Norman [31] 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 and rating scales, small sample sizes or data that do not follow a normal distribution. Following Norman, the analysis in this paper uses the mean and the ANOVA to illustrate differences between groups. However, we have also included the median as good practice.

For analysis of the free text questions, the answers were grouped up together according to common characteristics to allow for quantification. For example, synonyms such as "extortion" and "blackmail" were grouped together in the analysis. Each answer was counted separately in the cases where a respondent gave multiple answers to the question.

4. Demographics and Sample Description

This section describes the sample demographics and discusses representativity. The number of answers from the different questionnaires is: Slettmeg N = 24, Facebook/Twitter N = 198 and Reddit N = 107. Table 2 shows the response rate. The questionnaire was distributed to 123 customers of Slettmeg from April to May 2020. Reddit and Facebook were actively shared and posted for two weeks in May 2020. The number of possible respondents for Facebook consists of the number of friends from the people who shared the questionnaire. We approximated the number of people who had this information visible using the number of shares and average Facebook friends per share, Table 2. We rounded the number to the closest hundred. For Reddit, the table shows the number of members of the Norwegian subreddit r/norge, and the number of users that are usually online.

Table 2. Table showing answer rate with how many possible respondents there were on the platforms.

	Number of Possible Users	Achieved	Percent
Facebook/Twitter	4300	198	4.6%
Reddit Sub followers online users	133,000 1200	107	0.08% 8.9%
Slettmeg	123	24	20%

4.1. Sex, Age and Digital Natives

Table 3 illustrates that sex distribution varies greatly between the different platforms where the questionnaire was distributed. For example, the sample collected from Reddit has a very skewed sex distribution, with most of the people on the platform being male (88%). The sample from Facebook has 38% women, and the sample from Slettmeg has 54% women. This brings the total distribution to 68% men and 30% women in the sample. Comparing the sex distribution to the Norwegian population as a whole from Statistics Norway (SSB) (https://www.ssb.no/statbank/sq/10036277), 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. The dataset is biased towards males with an over-representation of 17%.

Table 3. Age and sex distributions sorted on recruitment platforms.

		Facebook	and Twitter		Reddit			Slettmeg				
		N	Row N%	Col N%	N	Row N%	Col N%	N	Row N%	Col N%	Tot N	Tot%
Age	<21	4	22.20%	2.0%	12	66.70%	11.2%	2	11.10%	8.30%	18	5.5
	21–30	108	60.3%	54.5%	66	36.9%	61.7%	5	2.8%	20.8%	179	54.4
	31–40	42	63.6%	21.2%	20	30.3%	18.7%	4	6.1%	16.7%	66	20.1
	41–50	25	69.4%	12.6%	7	19.4%	6.5%	4	11.1%	16.7%	36	10.9
	51–60	15	68.2%	7.6%	2	9.1%	1.9%	5	22.7%	20.8%	22	6.7
	61–70	3	50.0%	1.5%	0	0.0%	0.0%	3	50.0%	12.5%	6	1.8
	>70	1	50.0%	0.5%	0	0.0%	0.0%	1	50.0%	4.2%	2	0.6
	Total	198			107			24			329	100.0
Sex	Man	120	53.3%	60.6%	94	41.8%	87.9%	11	4.9%	45.8%	225	68.4
	Female	75	75.8%	37.9%	11	11.1%	10.3%	13	13.1%	54.2%	99	30.1
	No answer	3	60.0%	1.5%	2	40.0%	1.9%	0	0.0%	0.0%	5	1.5

The age distribution from the respondents can be seen in Figure 1 (numbers in Table 3). The numbers have an over-representation of people in the age group 21–30 from Facebook, Twitter and Reddit, this group also totals 54% of the sample. The Slettmeg-survey is more evenly distributed within the age groups. The second biggest group is 31–40 (20%) followed by 41–50 (11%).

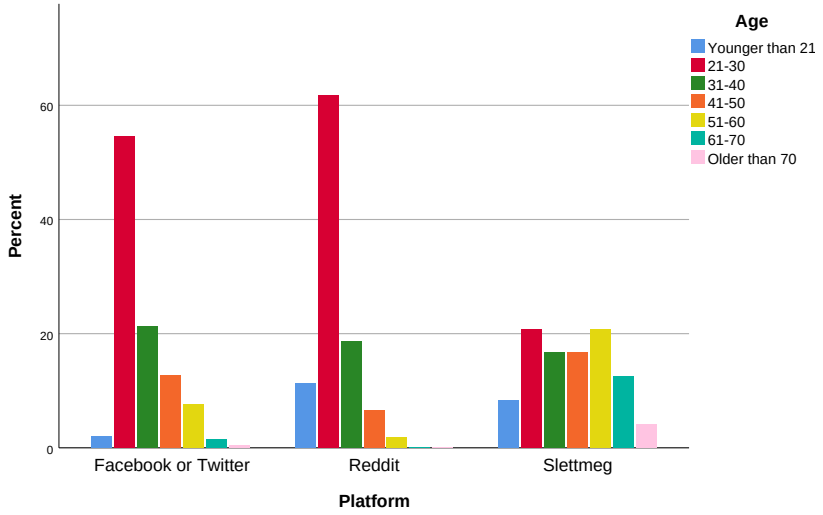

Figure 1. Comparison of age distributions, in %, for the different social media.

We split the age groups into two to investigate the digital natives-hypothesis [2], where natives are people born after 1987, see Table 4. The gender distribution within the groups is 71% males and 27% females in the digital natives group and 65% males and 35% females in the non-native group.

Table 4. Comparison of the number of digital natives and non-natives, sorted on gender and ID theft.

			Male		**Female**		**No Answer**	
			Count	Layer N%	Count	Layer N%	Count	Layer N%
Digital Native	Hacked account?	Yes	20	6.10%	12	3.60%	0	0.00%
		No	119	36.20%	41	12.50%	5	1.50%
Non-native	Hacked account?	Yes	6	1.80%	12	3.60%	0	0.00%
		No	80	24.30%	34	10.30%	0	0.00%

4.2. Further Sample Description

Norway comprises eleven counties, the distribution from the sample compared to the Norwegian population from SSB (https://www.ssb.no/statbank/sq/10036698) is visible in Figure 2. The difference between the population and the sample can mostly be seen with Oslo and Innlandet being over-represented, and Viken, Agder and Rogaland being under-represented.

Figure 3 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. SSB writes that 36.6% of the Norwegian population has higher education, compared to our sample where 79% reported to have higher education.

The people who participated in the questionnaire used the social media shown in Table 5. Since every person may use multiple social media platforms, the total amount displayed in the table exceeds the number of respondents of the questionnaire. From the table, we can see that there are at all ages, over 65% of people using Facebook as a social media platform. The numbers for Facebook keep climbing the older people get; with most of the other social media having a reverse distribution from Facebook. At least down to around the 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 the 41–50 group.

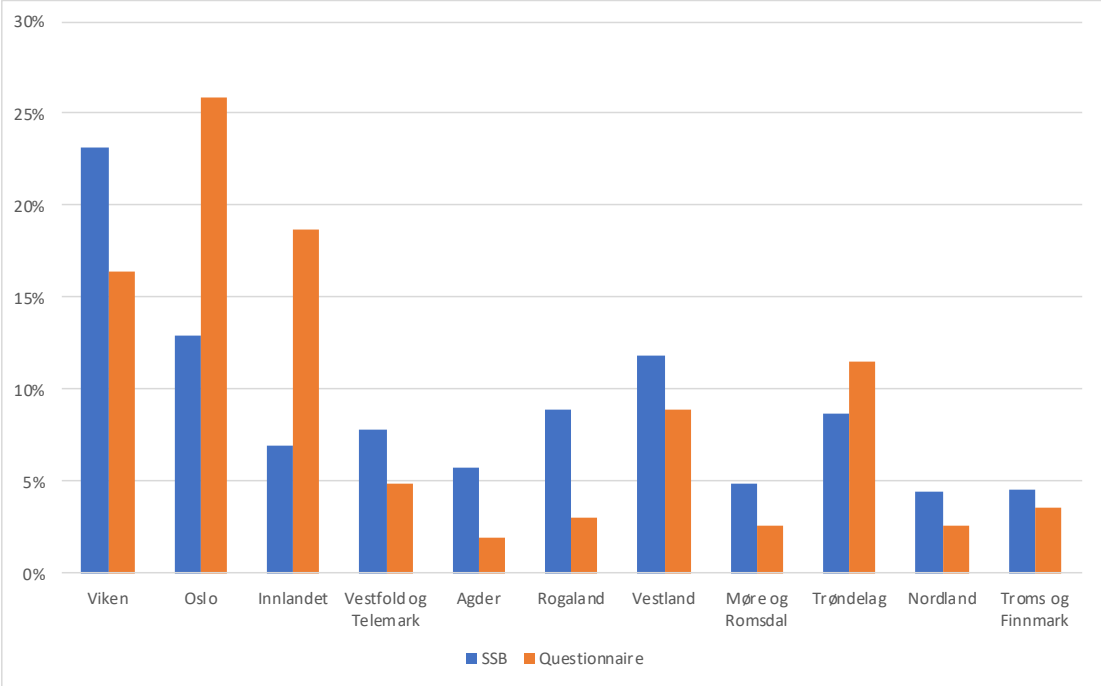

Figure 2. Comparison of municipality distributions, in %, the population based on data from Statistics Norway (SSB) vs. the questionnaire N = 305.

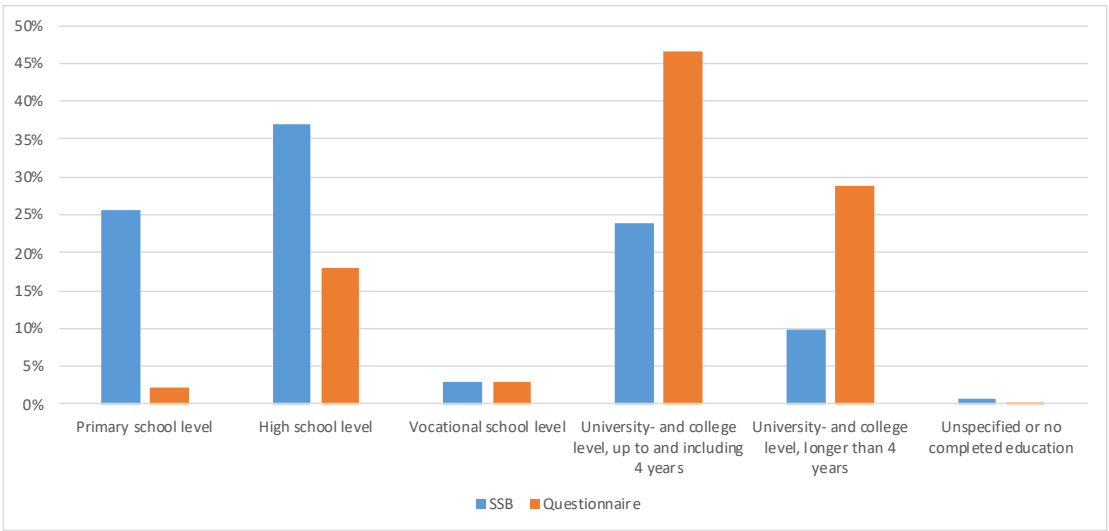

Figure 3. Comparison of education distributions, in %, of the Norwegian population based on data from SSB vs. the questionnaire N = 305.

The respondents of the questionnaire were also asked about how often they post on social media, as presented in Table 6. From the table, we can see that 53% of people post on social media more rarely than once a month. A total of 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 89% posting less than once a week.

Table 5. 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.

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 6. The table shows how often the respondents of the questionnaire post on social media. The total here is missing about 18 people, due to an unexpected error with the questionnaire.

	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	

4.3. Self-Assessment

We asked the respondents to rate their IT skills on a scale from *1—Very poor* to *4—Expert*. Figure 4 shows that only one person rates his IT skills as "Very poor". Furthermore, we can see that from both the questionnaire distributed on Reddit and Facebook/Twitter that around 15% of the respondents ranked their IT skill level at 2, this is in contrast to 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.

In Table 7, we can see how much people care about IT, information security and privacy: IT generally has a lower number of people caring about it. Information security and privacy are pretty similar in people's enthusiasm towards the subject. However, the respondents seem to care more about privacy.

There were no differences between the natives and non-natives in the self-assessment; however, there were differences between both the sexes and having been hacked, illustrated in Table 8: Where the respondents who had been hacked had a significantly lower perception of their generic IT competence. We see similar results for the females in the sample regarding IT competence, information security and privacy.

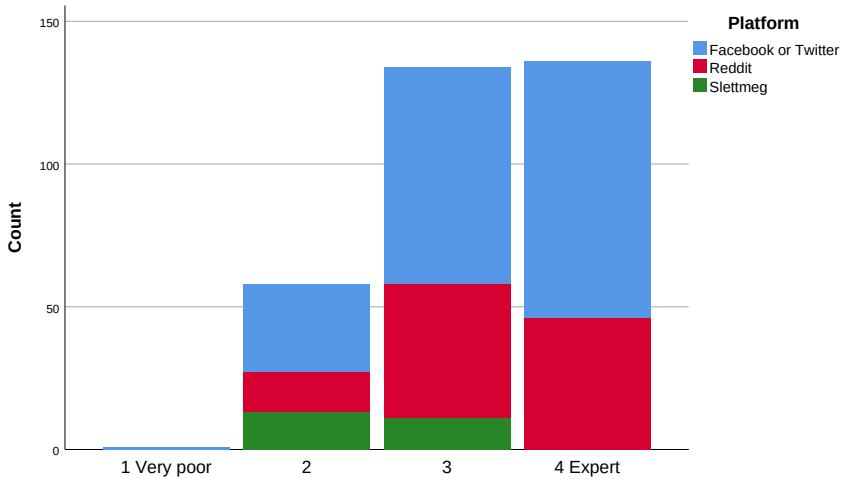

Figure 4. Comparison of self-reported IT skill, in %, for the different questionnaires N = 329. 1 was very little skilled, and 4 was highly skilled in IT.

Table 7. Comparison of self reported interest in IT in general, information security and privacy. The data are 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 caring a lot.

	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 8. Self-rating differences between the self-assessment categories.

	Category Hacket?	N	Mean	Std. Dev	Std. Error	95% CI Lower	Upper	Min	Max	Sig.
IT competence	Yes	50	2.9	0.735	0.104	2.69	3.11	2	4	
	No	279	3.29	0.728	0.044	3.2	3.38	1	4	
	Total	329	3.23	0.742	0.041	3.15	3.31	1	4	0.001
	Sex									
IT competence	Male	225	3.45	0.647	0.043	3.37	3.54	2	4	
	Female	99	2.69	0.665	0.067	2.55	2.82	1	4	
	Total	324	3.22	0.741	0.041	3.14	3.3	1	4	0
Information security	Male	225	3.33	0.732	0.049	3.24	3.43	1	4	
	Female	99	3.07	0.718	0.072	2.93	3.21	1	4	
	Total	324	3.25	0.737	0.041	3.17	3.33	1	4	0.003
Privacy	Male	225	3.33	0.749	0.05	3.23	3.43	1	4	
	Female	99	3.19	0.724	0.073	3.05	3.34	1	4	
	Total	324	3.29	0.743	0.041	3.21	3.37	1	4	0.127

5. Analysis and Results

The results are split into three major categories: Firstly, we analyse the differences regarding *security routines* on social media. Secondly, we investigate the *risk perceptions* of conducting different activities. Finally, we describe the risk perceptions of those who have suffered ID theft and the consequences they suffered. For each subsection, we describe the results for the groups as a whole, before describing the differences between the three groups (age, sex and ID theft).

5.1. Security Routines on Social Media

We present the security routines within the topics *update practices*, *password habits*, *privacy settings* and *visible information*.

5.1.1. Update Practices

We asked the respondents about their updating routines for the units they use to browse social media. Figure 5 shows that less than 52% of participants owned a tablet device, while 93% owned a PC/Mac and 99% of the respondents had a smartphone. We can see that most people update their devices as soon as they receive a notification about updating. Only 6% of the participants postpone system updates. The recommended frequency of how often one should update their devices is as soon as a patch is available, according to the Norwegian National Security Authority (NSM) (https://www.dn.no/teknologi/teknologi/datasikkerhet/microsoft/innlegg-sla-pa-automatiske-oppdateringer-unnga-datainnbrudd/2-1-654083). 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.

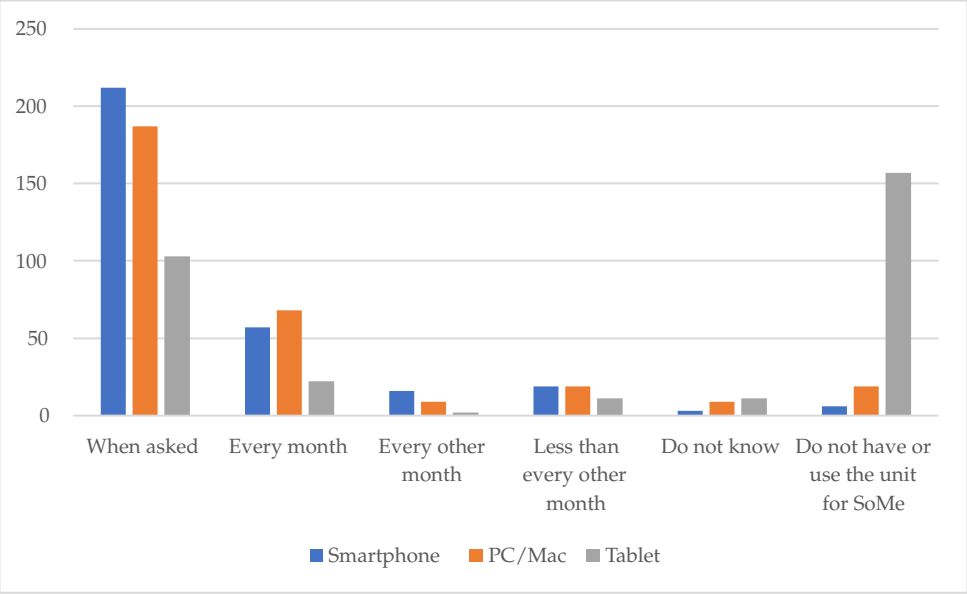

Figure 5. Shows in percentage how often respondents of the questionnaire update their devices. Mobile N = 313, PC/Mac = 311, Tablet = 306.

There were no differences between the natives and non-natives, genders or having experienced account theft when it comes to updating practices.

5.1.2. Password Habits

Passwords are what most services use to authenticate a person and give them access to their account on the site. Back in 2017, Thomas et al. [19] found that just from data leaks, 7.5% of credentials were still active and usable. We can see from the answers in Table 9 that the respondents probably

coincide with the number from Thomas et al. with 3% using the same password everywhere and 9.4% using the same everywhere, but applying 2-factor authentication if it is available. A total of 28.6% of the sample use variations of the same password on different sites to keep the passwords unique.

Table 9. Peoples answers on what their passwords habits are like N = 329.

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 different sites	94	28.60%
I always use different passwords	55	16.70%
I use different passwords and 2fa where possible	139	42.20%

There were no differences between natives and non-natives regarding password habits. There were differences between the sexes, where males seemingly have better password habits than females, Table 10.

Table 10. Differences in password habits between sexes.

	I Use the Same Password Everywhere		I Use the Same Password Everywhere, But Enable 2FA When Possible		I Use Variations of the Same Passwords on Different Sites		I Always Use Different Passwords		I Always Use Different Passwords and Enable 2FA When It Is Possible.	
	Count	Row N%	Count	Row N%	Count	Row N%	Count	Row N%	Count	Row N%
Digital Native	6	3.00%	14	7.10%	60	30.50%	31	15.70%	86	43.70%
Non-native	4	3.00%	17	12.90%	34	25.80%	24	18.20%	53	40.20%

5.1.3. Privacy Settings

In the questionnaire, the respondents were asked if they had changed their privacy settings. A total of 301 people said that they had changed their privacy settings to reduce exposure, and 28 people had left them as is.

Regarding the changing of privacy settings, we also asked to what degree that they had limited the visibility of their account N = 329, Figure 6. As seen in the figure, most people have limited the visibility of their information to a high degree. Furthermore, 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 the different privacy increasing measures that can 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.

Furthermore, when comparing the groups we find that the group that has suffered account hacking score consistently lower on all variables regarding visibility on social media, Table 11. Additionally, there are significant differences between natives and non-natives when we compare privacy settings on the variables *contact info* and *posts* with the natives having stricter settings. There are also differences between males and females on *friends and followers* ($p = 0.05$) and *profile visibility to search engines* ($p = 0.006$), with males having stronger restrictions on these variables.

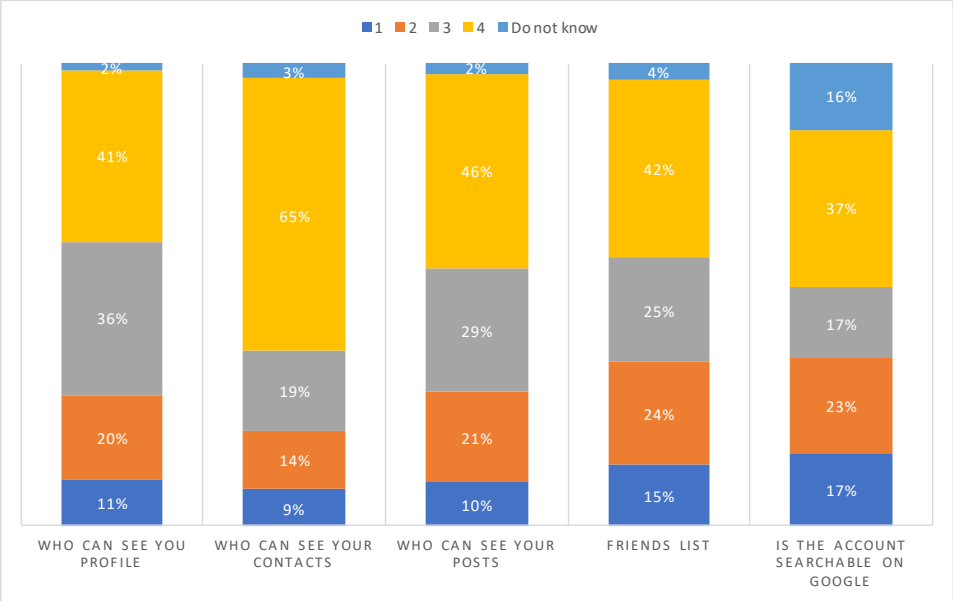

Figure 6. "I limit as much as possible who can see my ... on social media", answering "1" means no limitation on visibility, "4" means strict limitation on visibility and "0" means I do not know.

Table 11. Differences in privacy settings between sufferers of account hacking and the remaining sample. "I limit as much as possible who can see my ... on social media."

	Been Hacked?	N	Mean	Median	Std. Deviation	Std. Error	95% CI Lower	Upper	Min	Max	Sig.
Profile	Yes	50	2.6	3	1.195	0.169	2.26	2.94	0	4	
	No	279	3	3	1.005	0.06	2.89	3.12	0	4	
	Total	329	2.94	3	1.045	0.058	2.83	3.06	0	4	0.012
Contact info	Yes	50	2.94	4	1.3	0.184	2.57	3.31	0	4	
	No	279	3.27	4	1.084	0.065	3.14	3.4	0	4	
	Total	329	3.22	4	1.124	0.062	3.1	3.34	0	4	0.057
Posts	Yes	50	2.74	3	1.242	0.176	2.39	3.09	0	4	
	No	279	3.02	3	1.058	0.063	2.89	3.14	0	4	
	Total	329	2.98	3	1.09	0.06	2.86	3.09	0	4	0.097
Friends and followers	Yes	50	2.54	3	1.358	0.192	2.15	2.93	0	4	
	No	279	2.83	3	1.158	0.069	2.7	2.97	0	4	
	Total	329	2.79	3	1.193	0.066	2.66	2.92	0	4	0.112
Profile visibility to search engines	Yes	50	2.02	2	1.317	0.186	1.65	2.39	0	4	
	No	279	2.46	3	1.461	0.087	2.29	2.63	0	4	
	Total	329	2.4	2	1.447	0.08	2.24	2.55	0	4	0.046

5.1.4. Visible Information

We asked the people who answered the questionnaire what information they have visible on their social media platforms; the results can be seen in Table 12. It seems like the majority of the participants (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 personal data by Norwegian legislation (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/spesielt-om-sarlige-kategorier-av-personopplysninger-sensitive-personopplysninger-og-unntak/), people still have this information visible on their social media profile, in this case, 8.3% of the respondents.

Table 12. Shows how many people have what kind of information visible and the percentage based on the number of total respondents on the questionnaire 329.

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 overview	35	15.3%
Have hidden everything that I can	134	58.5%

There were only marginal differences between the natives and non-natives when we compare visible information. Non-natives are slightly more public with their email addresses ($p = 0.04$) and phone numbers ($p = 0.06$). The results also show that females also share information more openly about relationships ($p = 0.02$) and family members ($p = 0.01$), but the average scores for these two are still low, Table 13.

Table 13. What information do you have visible to the public on your profile?

	Category	N	Mean	Std. Dev	Std. Error	95% CI Lower	Upper	Min	Max	Sig.
Email	Digital Native	197	0.1	0.303	0.022	0.06	0.14	0	1	
	Non-native	132	0.18	0.387	0.034	0.12	0.25	0	1	
	Total	329	0.13	0.341	0.019	0.1	0.17	0	1	0.04
Phone no	Digital Native	197	0.06	0.23	0.016	0.02	0.09	0	1	
	Non-native	132	0.11	0.319	0.028	0.06	0.17	0	1	
	Total	329	0.08	0.27	0.015	0.05	0.11	0	1	0.06
Relationships	Male	225	0.15	0.359	0.024	0.1	0.2	0	1	
	Female	99	0.26	0.442	0.044	0.17	0.35	0	1	
	Total	324	0.19	0.389	0.022	0.14	0.23	0	1	0.02
Family members	Male	225	0.1	0.304	0.02	0.06	0.14	0	1	
	Female	99	0.21	0.411	0.041	0.13	0.29	0	1	
	Total	324	0.14	0.343	0.019	0.1	0.17	0	1	0.01

5.2. Risk Perceptions

One of the questionnaire's primary purposes was to measure risk perceptions while conducting certain activities and utilising social media. The questionnaire did not ask all the participants the same questions about all the different social media platforms; we did this not to tire out the respondents of the questionnaire. For example, we did not include the risk perception questions about Reddit on the questionnaire distributed on Facebook/Twitter, but we measured perceptions about Reddit for users of the service. For the analysis of the questions regarding the risk perception on social media, the N values for the platforms are as follows: Facebook N = 288, Twitter N = 134, Reddit N = 189, Snapchat N = 267, with a total of 329, illustrated in Table 14.

We document exact overlaps between use of SoMe services in the Appendix B, Table A1. A summary of the overlap in the sample is that having a Facebook account moderately correlates with having an Instagram (Pearson = 0.33) and a Snapchat account (Pearson = 0.34), there is also a moderate correlation between the two latter services (Pearson = 0.3). The survey was primarily

designed around sharing on Facebook, Twitter and Snapchat, so participants recruited from these platforms were not asked about risk perceptions regarding sharing on Reddit. For Reddit, the numbers used in the analysis are shown in the parenthesis (n = 107) in Table 14. Some of the categories are too small to draw conclusions about significance, especially females (11) and hacked users (13) on Reddit.

Table 14. Overview of categories distributed on the use of services.

		Facebook		**Twitter**		**Reddit**		**Snapchat**	
		No	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**	**Yes**
DigitalNative	Native	29	168	113	84	62	135 (78)	25	172
	Non-native	12	120	82	50	78	54 (29)	37	95
Sex	Male	38	187	124	101	61	164 (94)	53	172
	Female	2	97	70	29	78	21 (11)	8	91
	No answer	1	4	1	4	1	4 (2)	1	4
Hacked account	Yes	10	40	33	17	30	20 (13)	12	38
	No	31	248	162	117	110	169 (94)	50	229

5.2.1. Risk Perceptions on Social Media Posting

We asked the respondents about how they perceived risk when they posted various types of information on their social media accounts using the following rating scale: *1—Very low, 2—Low, 3—High* and *4—Very High*. Table 15 illustrates the results for all activities and platforms. The X-axis shows the count and percentage per answer per service. The right-hand side of the table shows a summary results in the form the mean for comparison. The *total average for topic*-line is the average of all the SoMe platforms for a topic for comparison of the total.

The results show that very few think posting images is a high-risk endeavour, all four services have a median of *2—Low*. Unsurprisingly, sharing photos on Snapchat is perceived to have the lowest risk being primarily a picture sharing service. Both Reddit and Snapchat have about 20% more respondents perceiving the risk of posting images as very low.

An example that has been seen is people having their houses broken into while on holiday, while it is uncertain that thieves use open sources to find victims or not, the threat is there and easily visible. We therefore attempted to gauge how people perceive the risks that can come from posting about a holiday on social media. 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.

Furthermore, pet names is a piece of information often used in security questions and we attempted to gauge how people perceive the risk of posting about something that very likely could show up as a security question on one of the services that they use. The results in Table 15 show that the Reddit and Twitter participants had the highest average with 25–27% perceiving the risk as 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 may be limited for the person posting such information on social media, it may be the answer to a security question of another person from the same household.

Another common activity on SoMe is to share content that the poster thinks is funny. The perceived risk of posting or sharing something humorous is highest on Twitter where 11% rate it as high and 2% at very high. Both Snapchat and Reddit have their very low perceived risk at around 50%.

Table 15. Differences in risk perception when posting various information on social media.

Topic		Very Low Count	N%	Low Count	N%	High Count	N%	Very High Count	N%	Mean
Post pictures	Facebook	55	19.10%	168	58.30%	55	19.10%	10	3.50%	2.1
	Twitter	22	16.40%	85	63.40%	22	16.40%	5	3.70%	2.1
	Reddit	39	36.40%	31	29.00%	24	22.40%	13	12.10%	2.1
	Snapchat	106	39.70%	127	47.60%	28	10.50%	6	2.20%	1.8
	Total	222		411		129		34		2.0
Vacation	Facebook	23	8.00%	128	44.40%	97	33.70%	40	13.90%	2.5
	Twitter	10	7.50%	44	32.80%	58	43.30%	22	16.40%	2.7
	Reddit	39	36.40%	31	29.00%	24	22.40%	13	12.10%	2.1
	Snapchat	65	24.30%	138	51.70%	44	16.50%	20	7.50%	2.1
	Total	137		341		223		95		2.3
Pets with names	Facebook	97	33.70%	147	51.00%	33	11.50%	11	3.80%	1.9
	Twitter	36	26.90%	65	48.50%	26	19.40%	7	5.20%	2.0
	Reddit	35	32.70%	43	40.20%	20	18.70%	9	8.40%	2.0
	Snapchat	124	46.40%	120	44.90%	17	6.40%	6	2.20%	1.6
	Total	292		375		96		33		1.8
Humorous content	Facebook	89	30.90%	164	56.90%	27	9.40%	8	2.80%	1.8
	Twitter	40	29.90%	76	56.70%	15	11.20%	3	2.20%	1.9
	Reddit	59	55.10%	43	40.20%	2	1.90%	3	2.80%	1.5
	Snapchat	129	48.30%	119	44.60%	15	5.60%	4	1.50%	1.6
	Total	317		402		59		18		1.7
Share news story	Facebook	92	31.90%	150	52.10%	40	13.90%	6	2.10%	1.9
	Twitter	30	22.40%	79	59.00%	22	16.40%	3	2.20%	2.0
	Reddit	57	53.30%	42	39.30%	6	5.60%	2	1.90%	1.6
	Snapchat	129	48.30%	119	44.60%	15	5.60%	4	1.50%	1.6
	Total	308		390		83		15		1.8
Share political opinion	Facebook	37	12.80%	127	44.10%	98	34.00%	26	9.00%	2.4
	Twitter	18	13.40%	52	38.80%	50	37.30%	14	10.40%	2.4
	Reddit	42	39.30%	42	39.30%	18	16.80%	5	4.70%	1.9
	Total	97		221		166		45		2.3
Participate in debate	Facebook	24	9.10%	97	36.60%	97	36.60%	47	17.70%	2.6
	Twitter	15	11.50%	42	32.10%	53	40.50%	21	16.00%	2.6
	Reddit	48	44.90%	39	36.40%	16	15.00%	4	3.70%	1.8
	Total	87		178		166		72		2.4
Use Snapmap	Snapchat	26	9.80%	77	28.90%	95	35.70%	68	25.60%	2.8

A common activity on SoMe is to share a news story with or without a comment. Table 15 shows how people perceive risk when sharing this information. Here, the combined high and very high comes to about 19% at the most (Twitter); this shows that very few people perceive the risk of sharing or posting news as high or very high. Between 52 and 59% rate the risk as low on Twitter and Facebook, 39% for Reddit and 47% for Snapchat, which is also the average and median. Between 48 and 53% perceive the risk as very low on Snapchat and Reddit.

Political opinion is considered as sensitive personal data in Norway. We asked the question about people posting or sharing something political to gauge if people find that exposing their political beliefs on social media can be risky/damaging. The results show that the users of Twitter and Facebook have the highest perception of risk with 43–48% rating it as high and or very high risk, both having the same average. Reddit is again quite far behind the other two social media with only is 22% on high or very high, this might again be because of the more anonymous nature of the Reddit as a social media.

Debating on social media can be risky, especially if one holds a political opinion that goes against the majority. In these cases, there is a real risk of cyber bullying and harassment.

The perceived risk of participating in a debate can be seen in Table 15. 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, while Facebook and Twitter are considered a lot riskier by the participants, both with an average of 2.6.

Snapchat was not considered an appropriate platform to share a political opinion or a debating platform and was left out of the survey for these two variables. However, we included one feature specific to Snapchat: We asked how people perceive the risk when using Snapchat's geographic location

service, Snapmap. Snapmap shows on a map where users were the last time they used Snapchat if they have this service activated. Figure 7 shows that the majority of the participants perceive snapmap as high risk (36%) or very high risk (26%). Which was also the information that was considered being the riskiest to share by the participants, with an average of 2.8.

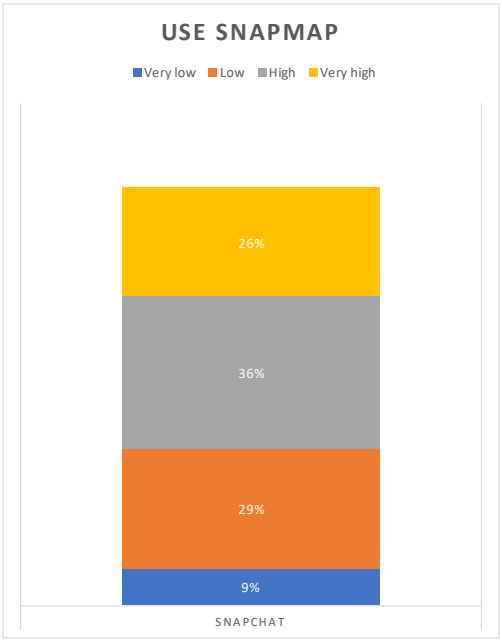

Figure 7. Shows how people perceive the risk of using Snapmap.

To obtain a result regarding which platform and activity is considered riskiest by the participants, we have aggregated the data in Table 16 averaging the result. The results show that Facebook and Twitter are perceived to be the riskiest platforms for sharing, while Snapchat and Reddit are perceived to have a lower risk. Furthermore, we see that using Snapmap is perceived as having the highest risk, followed by participation in debate, posting about vacations and sharing political opinions.

Table 16. The aggregated average risk perceptions sorted from high to low for the platforms and issues.

Platform	**Average**
Twitter	2.24
Facebook	2.17
Snapchat	1.91
Reddit	1.85
Topic	
Snapmap	2.8
Participate in debate	2.4
Post about vacation	2.3
Share political opinion	2.3
Post pictures	2.0
Pets with names	1.8
Share news story	1.8
Humorous content	1.7

5.2.2. Categorical Analysis of Risk Perceptions when Sharing on Social Media

We found that there were no differences in risk perception between the digital natives and non-natives considering all of the variables. Nor did having been hacked or suffering an ID theft influence the results. However, the differences in risk perceptions we found were between the sexes. Considering image posting, females consistently score higher than males across the Twitter, Reddit and Snapchat platforms, Table 17. The differences are minor and the median is the same, but the pattern is visible in the data. Females consider the risk to be higher for all platforms.

Table 17. Differences between sexes when posting things on social media.

Post Images	Category	N	Median	Mean	Std. Dev.	Std. Error	95% CI Lower	Upper	Min	Max	Sig
Facebook	Male	187	2	2.04	0.691	0.051	1.94	2.14	1	4	
	Female	97	2	2.11	0.776	0.079	1.96	2.27	1	4	
	Total	284	2	2.06	0.72	0.043	1.98	2.15	1	4	0.4
Twitter	Male	101	2	2	0.693	0.069	1.86	2.14	1	4	
	Female	29	2	2.24	0.577	0.107	2.02	2.46	1	3	
	Total	130	2	2.05	0.674	0.059	1.94	2.17	1	4	0.09
Reddit	Male	94	2	1.87	0.883	0.091	1.69	2.05	1	4	
	Female	11	2	2.45	0.82	0.247	1.9	3.01	1	4	
	Total	105	2	1.93	0.891	0.087	1.76	2.11	1	4	0.04
Snapchat	Male	172	2	1.66	0.643	0.049	1.56	1.75	1	4	
	Female	91	2	1.95	0.835	0.088	1.77	2.12	1	4	
	Total	263	2	1.76	0.727	0.045	1.67	1.84	1	4	0.02

Furthermore, when we analysed the remaining variables, we found seven more where females rank the risk as significantly higher than the males, Table 18. While the aforementioned results are the ones with significant differences, females only score higher on 4 out of the 26 variables where we measured risk perceptions (Table 15). Three are regarding pictures of pets on Facebook, Twitter and Reddit, while the final one is posting about holidays on Facebook. The difference in these four is also marginal.

Table 18. Differences in risk perceptions between groups on "How do you perceive risk when you conduct the following action on SoMe?".

Topic			N	Med	Mean	Std. Dev	Std. Error	95% CI Lower	Upper	Min	Max	Sig
Post about vacation	Snapchat	Male	172	2	1.99	0.806	0.061	1.87	2.12	1	4	
		Female	91	2	2.21	0.876	0.092	2.03	2.39	1	4	
		Total	263	2	2.07	0.835	0.052	1.97	2.17	1	4	0.05
Post pictures of pets with names	Facebook	Yes	40	2	1.6	0.709	0.112	1.37	1.83	1	4	
		No	248	2	1.9	0.767	0.049	1.8	1.99	1	4	
		Total	288	2	1.85	0.765	0.045	1.77	1.94	1	4	0.02
Post pictures of pets with names	Snapchat	Male	172	1.5	1.56	0.613	0.047	1.47	1.66	1	3	
		Female	91	2	1.78	0.8	0.084	1.61	1.95	1	4	
		Total	263	2	1.64	0.69	0.043	1.56	1.72	1	4	0.01
Share a news item	Twitter	Male	101	2	1.91	0.694	0.069	1.77	2.05	1	4	
		Female	29	2	2.21	0.675	0.125	1.95	2.46	1	4	
		Total	130	2	1.98	0.698	0.061	1.86	2.1	1	4	0.04
Share humorous content	Snapchat	Male	172	1	1.49	0.587	0.045	1.4	1.58	1	4	
		Female	91	2	1.82	0.739	0.077	1.67	1.98	1	4	
		Total	263	2	1.6	0.662	0.041	1.52	1.68	1	4	0
Participate in public debate	Facebook	Male	176	2	2.53	0.861	0.065	2.41	2.66	1	4	
		Female	85	3	2.8	0.884	0.096	2.61	2.99	1	4	
		Total	261	3	2.62	0.876	0.054	2.51	2.73	1	4	0.02
Participate in public debate	Twitter	Male	99	2	2.49	0.908	0.091	2.31	2.68	1	4	
		Female	28	3	2.93	0.716	0.135	2.65	3.21	1	4	
		Total	127	3	2.59	0.885	0.079	2.44	2.75	1	4	0.02

If we further examine the perceived risk of participating in a debate on social networks, we can see that one gender has a higher perceived risk than the other, Figure 8 illustrates the difference between groups for Facebook. Doing an ANOVA analysis on genders and risk perception on debates on both Facebook and Twitter gives us a $p = 0.02$. Other than fitting with the pattern of women rating the risks higher, the difference on Reddit is smaller and insignificant with $p = 0.1$.

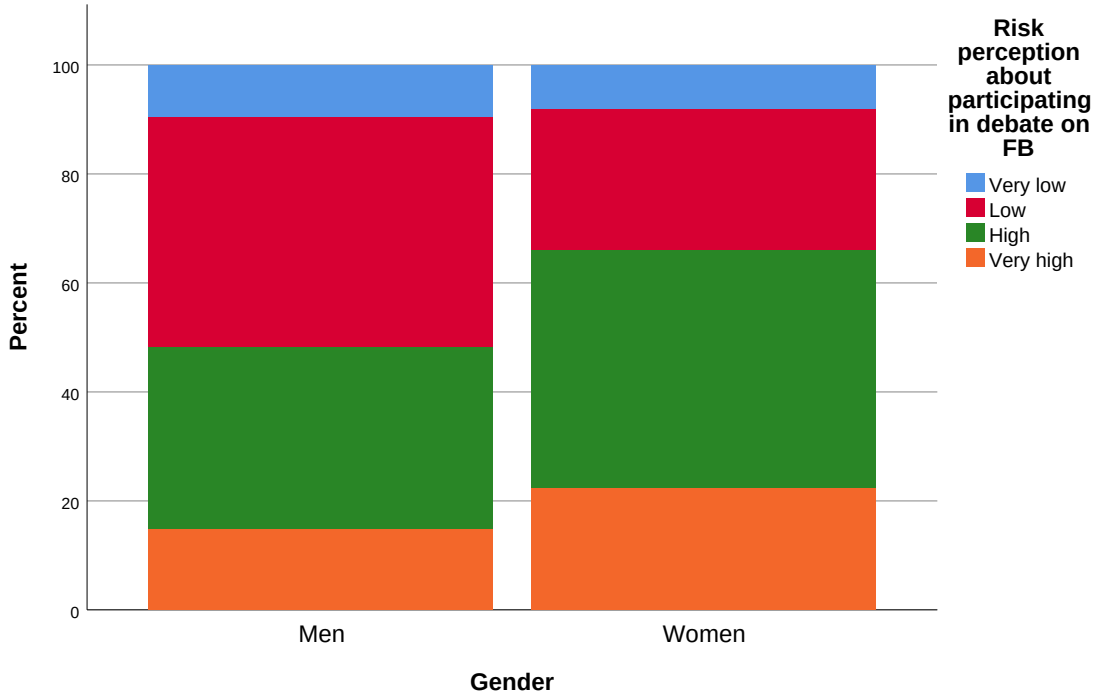

Figure 8. Shows how women and men perceive the risk of participating in debate on Facebook.

5.2.3. Perceptions on Information Exploitation in ID theft

The participants in the questionnaire were asked how they rate to what degree they thought that different information could be used to perform identity theft with the alternatives: *1—Very small degree*, *2—Small degree*, *3—Large degree* and *4—Very large degree*. The results can be seen in Table 19 where we have used the average to rank the information assets according to each other. 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 to a *very large degree*. In second place, we have debit/credit card numbers with 77.4% on very large degree. When we asked this question, we were 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 very large degree in regards to the information risk value, even though the social security number is not classified as sensitive data in Norway, and should, in theory, not let attackers abuse your identity by itself. How people rated the rest of the information points asked can be seen in Table 19.

Table 19. "To what degree do you think that your shared information can be abused in an ID theft?" N = 327–329.

Info Asset	Ranking	Count	Column N%	Average
Full name	Very small	45	13.70%	
	Small	156	47.60%	
	Large	89	27.10%	
	Very large	38	11.60%	
	Total	328	100.00%	2.4
Phone number	Very small	35	10.70%	
	Small	122	37.20%	
	Large	123	37.50%	
	Very large	48	14.60%	
	Total	328	100.00%	2.6
Email	Very small	33	10.10%	
	Small	128	39.10%	
	Large	116	35.50%	
	Very large	50	15.30%	
	Total	327	100.00%	2.6
Social Security Number	Very small	20	6.10%	
	Small	26	7.90%	
	Large	65	19.80%	
	Very large	218	66.30%	
	Total	329	100.10%	3.5
Date of Birth	Very small	28	8.50%	
	Small	127	38.70%	
	Large	120	36.60%	
	Very large	53	16.20%	
	Total	328	100.00%	2.6
Home Address	Very small	28	8.50%	
	Small	139	42.40%	
	Large	108	32.90%	
	Very large	53	16.20%	
	Total	328	100.00%	2.6
Bank account number	Very small	32	9.80%	
	Small	49	15.00%	
	Large	69	21.10%	
	Very large	177	54.10%	
	Total	327	100.00%	3.2
Credit card number	Very small	20	6.10%	
	Small	12	3.70%	
	Large	42	12.80%	
	Very large	254	77.40%	
	Total	328	100.00%	3.6
Health information	Very small	25	7.60%	
	Small	86	26.20%	
	Large	95	29.00%	
	Very large	122	37.20%	
	Total	328	100.00%	3.0
Account info and passwords	Very small	11	3.30%	
	Small	17	5.20%	
	Large	35	10.60%	
	Very large	266	80.90%	
	Total	329	100.00%	3.7

5.2.4. Differences in Perceptions on Information Exploitation in ID Theft between Groups

When comparing the groups, we find multiple differences. Starting with comparing the digital natives and non-natives, we find that there is a difference in how they perceive the risk, Table 20. The non-natives consistently rank the five information assets in the Table as higher risk of abuse than the natives. The largest difference between the groups is the view of date of birth, where the medians also differ. Two other information assets ranked higher by the non-natives are credit card numbers and passwords. The differences in the answers can be seen in Table 20, and it shows that about 9% of the digital natives think that the room for abuse is minimal if someone knows their debit/credit card numbers, similar to 10% for the account information and passwords.

Table 20. Categorical analysis of risk perceptions on information sharing.

	Age group	**N**	**Med**	**Mean**	**Std. Deviation**	**Std. Error**	**95% CI Lower**	**Upper**	**Min**	**Max**	
Social Security Number	Digital Native	197	4	3.37	0.953	0.068	3.24	3.5	1	4	
	Non-native	132	4	3.6	0.74	0.064	3.47	3.73	1	4	
	Total	329	4	3.46	0.88	0.048	3.37	3.56	1	4	0.02
Date of Birth	Digital Native	196	2	2.48	0.819	0.059	2.37	2.6	1	4	
	Non-native	132	3	2.78	0.885	0.077	2.63	2.93	1	4	
	Total	328	3	2.6	0.858	0.047	2.51	2.7	1	4	0.002
Bank account number	Digital Native	196	4	3.11	1.074	0.077	2.96	3.26	1	4	
	Non-native	131	4	3.33	0.932	0.081	3.17	3.49	1	4	
	Total	327	4	3.2	1.023	0.057	3.08	3.31	1	4	0.055
Credit card number	Digital Native	196	4	3.51	0.931	0.066	3.38	3.64	1	4	
	Non-native	132	4	3.77	0.6	0.052	3.67	3.88	1	4	
	Total	328	4	3.62	0.823	0.045	3.53	3.71	1	4	0.004
Account info & passwords	Digital Native	197	4	3.59	0.826	0.059	3.47	3.7	1	4	
	Non-native	132	4	3.84	0.492	0.043	3.76	3.93	1	4	
	Total	329	4	3.69	0.721	0.04	3.61	3.77	1	4	0.002
	Sex										
Phone number	Male	225	2	2.48	0.861	0.057	2.37	2.6	1	4	
	Female	98	3	2.7	0.864	0.087	2.53	2.88	1	4	
	Total	323	3	2.55	0.867	0.048	2.46	2.65	1	4	0.036
Email	Male	223	2	2.44	0.857	0.057	2.33	2.55	1	4	
	Female	99	3	2.78	0.84	0.084	2.61	2.95	1	4	
	Total	322	2.5	2.54	0.864	0.048	2.45	2.64	1	4	0.001
Date of Birth	Male	224	2	2.5	0.831	0.056	2.39	2.6	1	4	
	Female	99	3	2.82	0.85	0.085	2.65	2.99	1	4	
	Total	323	3	2.59	0.849	0.047	2.5	2.69	1	4	0.002
Home Address	Male	224	2	2.49	0.847	0.057	2.38	2.6	1	4	
	Female	99	3	2.7	0.863	0.087	2.52	2.87	1	4	
	Total	323	2	2.55	0.856	0.048	2.46	2.65	1	4	0.046
Bank account number	Male	224	3	3.05	1.049	0.07	2.92	3.19	1	4	
	Female	98	4	3.52	0.876	0.089	3.34	3.7	1	4	
	Total	322	4	3.2	1.021	0.057	3.08	3.31	1	4	0
	Hacked?										
Full name	Yes	50	2	2.58	0.971	0.137	2.3	2.86	1	4	
	No	278	2	2.33	0.835	0.05	2.23	2.43	1	4	
	Total	328	2	2.37	0.86	0.048	2.27	2.46	1	4	0.056
Email	Yes	49	3	2.8	0.935	0.134	2.53	3.06	1	4	
	No	278	2	2.52	0.853	0.051	2.42	2.62	1	4	
	Total	327	3	2.56	0.87	0.048	2.47	2.65	1	4	0.039

When comparing the sexes, the same pattern emerges as previously detected: The males and females perceive the risks quite similarly, but females rank all the 11 variables as slightly riskier than males. The significant differences are listed in Table 20. The biggest difference is for the bank account number, followed by email address and date of birth. Another interesting finding is that those who reported having suffered ID theft, reported the information assets full name and email address as higher than the rest of the sample.

5.2.5. Susceptibility to Phishing

The questionnaire had a section that attempted to measure susceptibility to phishing. The narrative that was presented was a typical malicious Facebook messenger message, and we asked how they would perceive it coming from typical social circles. The message that was shown to the respondents can be seen in Figure 9. Table 21 shows how people reported to react to the phishing message when asked if they would click it. The results show 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% from a family member, 4.1% from a friend and 1.3% from acquaintances. Furthermore, if we examine the *maybe* answers, we also see that these are lower for the acquaintances than for the others. The numbers might be lower than what is expected with this being self-reported, but that would probably skew the numbers towards the lower end of the scale, and the success rate might be higher.

Figure 9. Example of Norwegian phishing message that has been circulating from hacked Facebook accounts and sent to people on their friends list.

Table 21. Who the respondents thought they might get tricked into clicking a link if they received it from. N = 314.

	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%

We found no differences between the sexes or age groups for these variables, but for the group that had suffered ID theft reported to be more trusting of messages received from family

and close family. Even though the ID theft group represents only 15% (48 of the 314 total) of the sample, they are over-represented in both the *yes* and *maybe* categories for both the Family and the Close family variables. Only 5 out of 13 of the *yes* answers in the family and 6 out of 19 in the close family variable are from the hacked-group, 38% and 31%, respectively. The differences are visualised in Figure 10 where each bar on the x-axis counts as 100% to illustrate the difference.

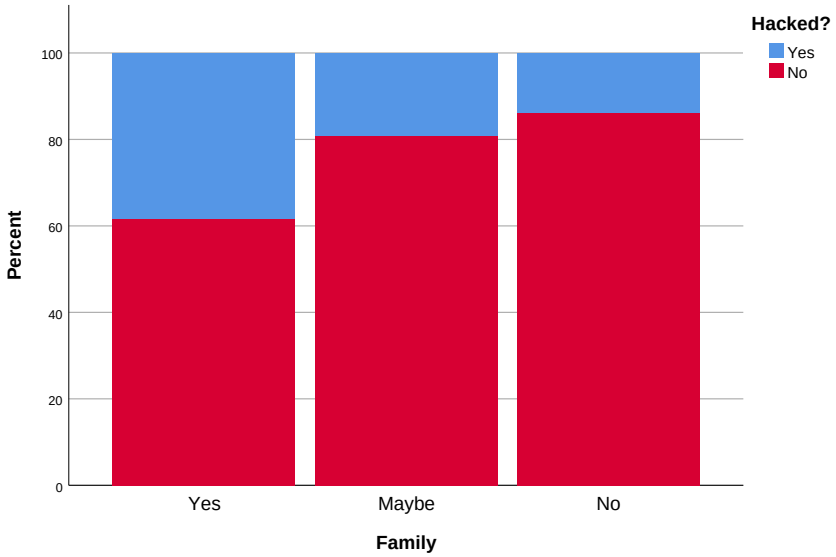

Figure 10. Susceptibility to clicking phishing messages coming from a family member sorted on those having suffered ID theft.

5.3. The Consequences of ID Theft

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 22. As we can see from the table, 14.3% of the respondents of the questionnaire have been hacked and got their accounts back, 0.9% have been hacked and have not got their account back and 84.8% of people have not experienced having their account on social media compromised. Table 23 shows the demographics of the 50 participants that have suffered ID theft, where there are 52% males and 48% females and 64% and 36% non-natives. There were no clear patterns regarding age in this group, but when we consider sexes, the distribution of the sample as a whole was 30% females and for the hacked account group it was 48% indicating an over-representation for this group. Theses respondents that had experienced being hacked got some further questions about their experiences from having their accounts compromised.

Table 22. Shows the number of people who have had their account hacked.

		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 23. Demographics of users who had suffered ID theft and account hijacking.

	<21	21–30	31–40	41–50	51–60	61–70	>70	Total
Male	2	18	2	0	3	1	0	26
Female	1	11	4	5	2	1	0	24
Total	3	29	6	5	5	2	0	

5.3.1. Reason for Compromise

We asked the respondents how they thought they got their account compromised with alternatives. Table 24 shows what people thought were their reasons for compromise N = 47. The hacked option represented the broadest category and was chosen by 15 respondents. It is hard to know if the reason to compromise is the reuse of a password or a weakness in the platform used.

The questionnaire also had higher granularity options, and a written option: The results show that eight people, or about 17% of the people had their accounts compromised because of falling for a phishing scheme. Two people chose the *Shared the password with someone in my close relations* as the cause, both of these happened to a digital native. For the people who chose other, one wrote that he had his account compromised by a Keylogger, one had been compromised through brute force attack and the last one attributed the hacked account either to a keylogger or a remote access tool. Nineteen (40%) answered that they did not know how it happened.

Table 24. Stated reasons of account compromise. N = 47.

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

5.3.2. Consequences of Social Media ID Theft

We asked the respondents about the consequences they had suffered because of the ID theft. The question had a free text open answer, and we have categorised and quantified the overall answers in Table 25. The main result is that 65% of the respondents were not able to attribute or find out exactly why their account was hacked and did not suffer any consequences. The respondents had difficulties answering how their accounts had been abused. When they managed to attribute what the hackers did, it was usually because they used the account for spam (10%) or phishing (8%). To be more specific, 10% of people experienced the consequence that their account was used to send out spam messages, and 8% of people had the account send out phishing messages or that the account was used in other phishing campaigns. A total of 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. Another re-occurring topic in the answers is that several who got hacked were quick to regain control of the account: several of the written responses detail that the ID theft had negligible consequences because it got detected immediately primarily through a "log on from new device" email notification. This security mechanism allowed them to respond quickly to the event and mitigate the consequences.

Analysing the sample, none of our respondents suffered very serious consequences from the ID theft, such as for example, being swindled for large sums of money or being severely exposed or harassed online. However, the sample does contain descriptions of serious consequences: One respondent describes being locked out from her Facebook and Instagram accounts, both of which were corporate accounts. She also got exposed online through the hack and describes the experience as traumatising. The consequence was that she locked down her accounts and stopped her online initiatives. Another respondent had his account abused by the hacker for buying and selling items. The respondent did not detail his answer beyond writing that *"It created problems for me"*. Account lockout with the additional workload to regain control described as the primary consequence.

Table 25. Shows categorized reasons for compromise from text answer in the questionnaire. The reasons have been grouped a bit together with other similar consequences N = 40.

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%

The group who answered that they had not experienced having their social media profile hacked was asked how they thought a compromised social media account could be abused. This was a voluntary question which received 197 answers, whereof some respondents answered multiple consequences which were counted individually. Table 26 shows that 40 respondents answered *impersonation/ID theft* as the consequence of a compromised social media account, here the users talked about their profile being used for malware spreading or other nefarious acts that tries to portray the hacker as them. Typically referred to as a *masquerade attack* in the literature. *Manipulation* is people talking about either the account used for sharing of propaganda or sharing of fake news.

Table 26. Grouped open answers that a compromised account can be used for. N = 205.

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

Active account abuses such as *spam* (26), *spread malware* (23) and *phishing* (17) follow as the most commonly perceived consequences. These are instances where the attacker abuses the hijacked account to attack others. Further down the list, we find consequences such as *swindling* and *blackmail* which are primarily motivated by financial gain. Another interesting perceived consequence for financial gain is *follower farming*, where the attackers gather multiple compromised accounts on a given SoMe platform and sells followers to potential buyers who are looking to increase their following.

5.3.3. Activated Measures

We asked the respondents who had had their social media account compromised what measures they had implemented to increase the security of their account post-compromise; the controls implemented can be seen in Table 27. 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. From Table 27, we can see that the most popular measure to apply is 2-factor authentication 32, and notification on suspicious behaviour 29. After that comes starting to use passwords longer than 12 characters 22 and having the firewall turned on 15. A total of 13 people started changing their passwords regularly, 11 started using an anti-virus and 9 people took other measures. Five people have changed their passwords to a password shorter than 12 characters.

Table 27. Measures users who have had their accounts compromised have activated to help mitigate a new compromise. N = 47.

Measures	Count
Activated 2 factor authentication	32
Activated notification on suspicious behaviour 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

One respondent commented on the efficiency of two-factor authentication: *"I approximately get two text messages each month about log in attempts at Facebook using my username and password, but they can not get in because I have activated two-factor authentication..."*

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 28, we can see that most of the people who have incorporated regular password changes into their security practices change their passwords every third month. Seven people started 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.

Table 28. Shows how often the people who had decided to use regular password changes as a control changes their passwords. N = 13.

Password Change Frequency	Count
Every third month	7
Every month	3
More frequent than once a month	1
Every six moths	1
Every year	1
More infrequent than every year	0

6. Summary of Findings and Discussion

In this section, we discuss the findings with regards to the research questions, starting with sharing habits and exposure to ID theft. We discuss the findings on risk perceptions of ID theft on SoMe. We also discuss the differences and similarities between the analysed groups to answer the outlined hypothesizes. Finally, we discuss the findings regarding how ID theft occurs and the consequences of said event.

6.1. Sharing Habits and Exposure to ID Theft on Social Media in Norway

We started by exploring the update practices for the sample and found that the majority of the respondents updated their devices when asked by the operating system. Moreover, very few waited longer than two months to update their devices. For the generic assessment of password security, we also found that only 3% chose the weakest alternative *"I always use the same password for everything"*, while 29% used a password rule with small variations of a password on different sites. Using different passwords and enabling multi-factor authentication are both considered strong practices. There were no differences between the groups in this area.

The results were similar when we examined the limitations and restrictions the respondents put on the visibility of their account information, where the results show that the majority of the respondents put limitations on what they share on their profile. Between 54 and 84% of the answers fell into either 3 or 4, where the latter means as strict limitations as possible. Furthermore, we found that 58% had hidden everything that they could when we asked what information they had visible on their SoMe platforms. The results show that the sample as a whole was security-aware.

When we examined differences between the groups, we found differences between the digital natives and the non-natives in the analysis: The digital natives had stricter *privacy settings* on *contact info* and their SoMe *posts*. We also found this pattern when we examined the information the groups had visible on their profile, whereas non-natives were slightly more public with their contact information such as email addresses and phone numbers. Contact information is generally viewed as public information in Norway and is commonly listed in the Yellow pages; the personal risk assessment of sharing this information might be reduced over time.

Considering the differences between the sexes on the sharing issues, we found differences between males and females on sharing their *friends list* and their *profile visibility to search engines*. The pattern here was that males had stricter privacy settings. Furthermore, the results also showed that females share information more openly and share about relationships and family members. However, the scores for these variables were still low, and the differences were that females were slightly more open on their privacy settings and visible information.

The group we were the most curious about was those who had suffered ID theft, and how this affected the security routines. When we analysed limitations on SoMe information, the group that had suffered ID theft scored lower on average across all of the five measured variables (Table 11). Although the difference was minor in three of the five variables, the pattern was evident for this group. A hypothesis for future work could be to examine the relationship being exposing information and the risk of ID theft.

6.2. Risk Perceptions of Social Media Use

When we examined the risk perceptions of social media usage, we started by analysing the risk perceptions of posting various pieces of information on SoMe. The survey design was such that choosing a specific SoMe triggered questions about it. We compared the actions on Facebook, Twitter, Reddit and Snapchat. As an aggregated result, we found that the respondents considered Facebook and Twitter to be riskier than Reddit and Snapchat. This results might be due to Twitter being an open platform where everyone can read content unless one has strict privacy settings. However, the information on Facebook is arguably less accessible than Twitter as it has more protection by

default than Twitter, but the results have these two close together. The risk perceptions of conducting activities on these two services follow each other closely (Table 15), except posting about vacation, which is deemed a somewhat higher risk on Twitter than Facebook.

Reddit does not use real names by default and provides a level of anonymity for its users. This feature is likely the reason that it received the lowest overall risk score across all the measured variables except posting pictures and pets with names. Images can contain quite a bit of metadata which can be abused to figure out information about the camera and where the picture was taken (geo-tagging). This information can 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 are vulnerable. Information also become mostly public once it is posted on the forum. We assume that there are many highly competent IT users on Reddit, and the combination of these issues might be the reason why posting pictures is perceived as risky by the Reddit users. A note on sharing information shared about pets is that it, in some cases, easily can be abused to break security questions. In our comparison, Reddit has the lowest overall risk.

Examining Snapchat shows that it is close to Reddit in the overall score. Generally, sharing information on Snapchat is deemed to have a low risk by our participants. However, Snapchat also has the riskiest function, which was Snapmap. Snapchat also provides a level of anonymity on a username level, but using it for sharing pictures severely weakens the anonymity of the service. Snapchat has the lowest risk score for posting pictures, which makes sense as it is primarily a picture sharing service. Snapchat allows for strict control of who gets to see the shared information and, to the user, the data seems to disappear after a brief period. These are likely explanations of why Snapchat is deemed more secure as a whole. However, is there grounds for considering Snapchat as more secure for posting pictures than the other services? There are some further answers in the data to this question: Considering the results in Table 15, each activity is ranked according to the platform on which it is conducted. Table 16 provided the aggregated results of both platforms and activities. Considering the activities, we can induce the information assets and threats for each and propose a threat model, Table 29. For example, if the main concern is stalking or burglary, the Snapmap would be the riskiest service as it reveals the location to potential stalkers and burglars. Expanding on the burglary risk, the secondary asset at risk would be valuables located at the property. Participating in an online debate is considered to be risky by our participants. This activity often reveals the political opinion of the debater, and this information is, in many cases, considered as sensitive personal information.

Furthermore, a debater exposes himself/herself to the public, and controversial opinions can have severe consequences if one gets targeted by the mob. Sharing a political opinion is similar to participating in debate, but often with less exposure. Our sample deemed these two activities as equally risky. Sharing a news story was mostly considered a benign activity by the respondents; however, most SoMe users have encountered the spreading of fake news online. Sharing news stories can also reveal political opinions.

From the categorical analysis of the issue, we found that females consistently rank risks higher for the majority of the measured activities. This finding is consistent with previous work on risk perception between men and women, where women express far greater concern than men about risks and hazards [8,32].

When asked to what degree specific information assets could be abused for ID theft, there were three that were ranked higher than others: *account information and passwords*, *credit card numbers* and *social security numbers*.

There were differences between the digital natives and non-natives, where the non-natives ranked five information assets as higher risk of abuse. These five included the three overall highest risk assets mentioned earlier. There can be several causes for this difference. Given that a portion of the natives are in their early twenties, they might not have as much capital at risk when considering abuse of credit card numbers. The value of account information and passwords may also increase over time, with the non-natives having accumulated more wealth, responsibility and higher risk. Understanding

of technology may also be a factor in risk perception as better understanding of systems should lead to a more calibrated risk judgment. Previous studies have shown that natives tend to have increased confidence regarding technology [2].

Table 29. Proposed threat model for social media (SoMe) activities.

Topic	Risk Score	Exposed Information	Threat
Snapmap	2.8	Location and whereabouts	Stalking/Burglary
Participate in debate	2.4	Political views, opinions, standpoints	Harassment and bullying
Post about vacation	2.3	Location and whereabouts	Stalking and burglary
Share political opinion	2.3	Political views, opinions, standpoints	Harassment and bullying
Post pictures	2.0	Personal information	ID theft / Exposure
Pets with names	1.8	Personal information	ID theft/Account hijack
Share news story	1.8	Political views, opinions, standpoints	Being manipulated/Fake news
Humorous content	1.7	Political views, opinions, standpoints	Harassment and bullying

The difference between sexes are consistent with the previous results in this paper, as females rank all of the 11 variables as slightly riskier than males. An interesting finding is that the group that had suffered ID theft or account hacking ranked the variables *full name* and *email* as more risky. This information is generally considered open, but having suffered an incident seems to change the perception of this issue.

We also attempted to measure susceptibility to phishing attacks presenting the respondent with a common attack method employed in SoMe. This task attempted to measure how trust influence decision making in SoMe. The task hypothesizes that a message from an acquaintance has a lower probability of being clicked than from a person in close social circle. The results show differences, but more than 84% of the respondents answered *no* for all four options. The probability of clicking the link was highest if received from the close family group (6%), which is a low number, but high enough for these scams to succeed. If between 1 and 5% click the link and get compromised, these attacks will propagate quickly through SoMe. Our results also show that the group that had suffered ID theft were more trusting, which adds to the trend for this group of having slightly weaker security controls.

These differences of risk perceptions are a potential path for future work.

6.3. How does ID theft Occur and What are the Consequences?

This study had 50 participants who reported to have had their accounts compromised. This group ranked their IT competence as significantly lower than the remaining group (Table 8). The results showed that as a cause of compromise, the majority chose either the *do not know* (19) or the *hacked* (15) option. The *hacked* option is too broad to draw any conclusions. However, a phishing attempt had fooled eight, and two reported to have shared their password with someone in their close relations as the cause. Keyloggers (malware) had compromised two participants, and one participant wrote that a brute force password cracking attack was the cause.

The hacked account group consisted of 52% males and 48% females, which indicated an over-representation of females in this group compared to the sample as a whole. However, not if we compare to the Norwegian population as a whole. The group of 50 is not large enough to draw any conclusions, but this finding also aligns with previous work in Nyblom et al. [20] where the hacked account owners also had an over-representation of females. Furthermore, comparing to the results in Nyblom et al., we find that phishing and malware infections are common causes. Weak password security is a re-occurring topic in account hacking, and we see varying practices within this area as well. Two respondents had gotten compromised by telling the password to someone. However, if we take into account the results from Thomas et al. [19] and Nyblom et al. [20], in which both had

password reuse as a common cause, we can assume that a large portion of the *hacked* group too got hacked through password reuse.

The majority of the respondents did not suffer any severe consequences from the compromise. The most severe was an abuse of corporate accounts followed by psychological consequences and a withdrawal of SoMe. Additionally, one participant had his account abused for buying and selling. Table 25 illustrates that compromised SoMe accounts have a broad potential for misuse. *Spamming* and *phishing* were the two most frequent forms of abuse. Both are a form of impersonation where the attacker exploits the SoMe account to distribute messages. Spamming is a way for the hacker to try to exploit the trust between two parties for financial gain, while phishing leverages the trust to harvest more credentials or credit card information. Two accounts were abused for blackmailing.

Although we were only able to interview two sufferers of ID theft, we found that in one case, the hacker used their business account on social media to buy ad slots on the platform. There can be big money in scam ad campaigns for hackers (https://www.cnet.com/news/your-hacked-facebook-account-may-be-bankrolling-scam-ad-campaigns/).

Of the more severe consequences, three 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 behaviour, or if it was the hackers that were performing some denial of service.

The presented findings align with the findings from asking the participants who had not suffered an ID theft what they thought would be the consequences, Table 26: Impersonation was a major concern, followed by spamming, spreading malware, phishing. Stealing money, swindling and blackmailing were also among the perceived consequences. Destroying reputation was also a commonly perceived consequence. The results illustrate that the majority of the participants were aware of the risks posed by ID theft.

The results also document that several of the respondents benefited from having the notifications of new logins feature enabled. This mechanism allowed for a swift response to the compromise and mitigation of potential consequences.

7. Conclusions

This paper has focused on the Norwegian population, exploring how people perceive risks arising from the use of SoMe, focusing on the analysis of specific indicators such as age, sexes and differences among the users of distinct social media platforms. Some differences across the examined indicators were noticeable, most notably, that the group that had suffered ID theft had weaker security controls which may have increased their exposure in the first place. Furthermore, the results document differences in risk perception when using the four different SoMe platforms, where Reddit and Snapchat are considered as safest, and Facebook and Twitter as most risky. The riskiest activity on SoMe is considered to be using the Snapmap followed by debate participation. Additionally, there were consistent differences between males and females, where females consistently ranked the risks as higher. There were no differences between the age groups considering SoMe activities, but non-natives ranked the risk of sharing the most critical information assets as higher. Finally, considering our sample, having suffered ID or account theft did not influence risk perceptions on performing SoMe activities, but the participants perceived higher risk of sharing certain information assets. To summarise, the measured security routines in the sample were generally healthy, and the majority of participants seemed to have a sufficient understanding of security risks and awareness.

7.1. Study Implications

This paper explored the areas regarding different SoMe platforms and how people perceive risk when doing different activities on SoMe. It also looked at this issue in context with people who have had their accounts compromised. The study documents that the study participants consider uttering their political positions and participating in debates as very risky. This issue was prevalent on Facebook

and Twitter, and especially females considered this as a high-risk activity. SoMe are political arenas, but our results document that many citizens dread participating because of the possible ramifications. Future research should study the implications of this finding in-depth, possibly together with the effects of cyber-bullying.

Our study further implies that suffering an ID theft changes risk perception within certain areas: such as valuing personally identifiable information like full name and email higher. We found the most significant differences when we looked at the sexes, where females generally perceived higher risk than males. This finding might imply that fewer females participate in discussions on SoMe platforms. Although the difference in risk perception between sexes is well-known, how it impacts participation in discussion and debates is not widely studied.

One of the measures that people chose to activate to secure their account were notifications on suspicious behaviour. Our results also showed that several who had their SoMe accounts compromised managed to take actions due to login notifications quickly. They managed to take mediating action before the hackers could do any noticeable harm. An implication here is that time is of the essence when dealing with hacked accounts and being able to regain control quickly is important for damage limitation. This finding was unexpected and warrant further research into the efficiency of account security mechanisms.

If we look at the proposed threat model for the different risks around sharing, we saw that Snapmap was the risk that people perceived as the worst, followed behind by debating, posts about vacation and sharing political opinions. We deduced that stalking, burglary, harassment and bullying were the primary concerns of the participants. This assessment needs further validation studies and can be used for understanding the risk perception of the user in future designs.

The study shows that some SoMe platforms are seen as higher risk than others, by their users. Facebook and Twitter have the highest aggregated risk, and are both quite a bit above Snapchat and Reddit. Both Twitter and Reddit are generally open SoMe platforms where everyone can see each others posts. The implication from this is that the privacy a closed SoMe like Facebook offers does not reduce the perceived risk when compared to a more open platform like Twitter, where everything is open and no invitation is needed.

7.2. Limitations

Although we do not know what the real demographic looks like for Norwegian SoMe users, we have some clear biases in the sample: 75% of the sample comes from the age group 21–40. The age distribution is highly skewed towards the younger generations. The majority of the sample was also males (68%). These two over-representations are most likely an effect of the participant recruitment strategy that utilized Facebook and Twitter through social media profiles to sample the general population. Many people from the age groups of the authors (20–40) answered the survey, which reflects the social network demographic and outreach of the authors. This difference might stem from a sampling bias caused by most of the sampling happening trough our social media network and receiving help with sharing the questionnaire from our existing network. The respondents also have a higher than average educational level, which might skew the risk perception a bit if a lot of the people who answered the questionnaire might have a more straight forward understanding of risk, with risk solely being consequence times probability of an event happening; like Slovic [27] mentioned, there are differences in how laypeople and experts define risk. The discrepancy in counties 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. The sample has a representation from all the Norwegian counties, with a slight over-representation from the central/eastern counties. We do not expect county representation to have any impact on the results as the expected variance in culture is negligible.

The over-representation of males was not perceived as an issue in the analysis as the data contained answers from 99 females which is a large enough sample to conduct analysis. Furthermore, the age groups were split into digital natives and non-natives as this provided large samples for

testing. Optimally, the results would have contained enough respondents for each age group to test for significance. Furthermore, another issue that needs to be discussed is the low response rates which are inherent to similar studies. Thus, although the number of responses is sufficient for the purposes of this analysis, we do notice a low response rate, down to 0.08% for Reddit, which are indicative of the difficulties to establish engagement with the general population.

7.3. Future Work

We mentioned some possible venues for future work under *limitations*; besides, we propose the following venues: Figure out if some hacked social media accounts are being used for different things than 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 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 venue could be if and how risk perception influences willingness to share their opinion and self-censorship, considering the consequence of participation as 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? To get some more insight into this, one could ask people to rate how anonymous they find the given social media. This could have been an interesting data point that could have shone some more light on why some things are perceived as less risky than others. This point might have given some insight into why some social media platforms perceive the risk of posting/sharing as lower than others.

Additionally, more knowledge can be gathered regarding account abuse: In this study, we attempted to get insight into this with the questions about consequences. However, 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. We failed to get enough ID theft sufferers into an interview, but this is still an interesting venue for further research.

More research could also be done in the risk perception and security routines of hacked users. The questionnaire shed some light onto this demographic. However, recruitment could have been better, and this aspect would have benefited from some qualitative interviews, where one could really prod at how their security routines look.

It could also be interesting to explore the reasons for the discrepancy in risk perception between the hacked and non-hacked population: is there a special reason for why people who had been hacked had a lower perception of risk? Was it because they were hacked, or was the hacking a product of their low perceived risk?

Another point of interest could also be to look into why there is a difference between natives and non-natives in what information they perceive to have the highest risk associated with it.

Author Contributions: Conceptualization, P.N., G.W. and V.G.; methodology, P.N., G.W. and V.G.; formal analysis, P.N. and G.W.; investigation, P.N., G.W. and V.G.; data curation, P.N. and G.W.; writing—original draft preparation, P.N., G.W. and V.G.; writing—review and editing, P.N., G.W. and V.G.; supervision, G.W. and V.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: Authors acknowledges the contributions made by NorSIS and Slettmeg.no by lending their resources to our disposal. We also thank everybody who helped distribute the questionnaire and recruit participants. We also want to thank the participants who took the time to participate in our study. Finally, we thank the anonymous reviewers for help with improving the paper.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Questionnaire

Nr	Category	Question	Type	Alternatives	Measure
1	Demographic	Age	Category	10 year ranges	Biases in sample
2	Demographic	Sex	Category	Categories	Biases in sample
3	Demographic	County	Category	Norwegian counties	Biases in sample
4	Demographic	Education	Category	Standard	Biases in sample
5	Self-assessment	On a scale from 1-4, how competent are you in ICT?	Scale	1 – very low competence/ 2/ 3/ 4 – Expert	Perceived competence
6	Self-assessment	(Matrix) How much do you care about 1. IT in general 2. Information security 3. Privacy	Matrix with scale	1 – Very little / 2/ 3/ 4 – Very much	Interests in security related topics
7	Social media presence	Which social media do you use?	Checkbox	Facebook/ Instagram/ Twitter/ Reddit/ TikTok/ Snapchat/ Others	Amount of SoMe accounts
8	Social media presence	If the respondent clicked "Other" in Q7.	Textbox	Free text	
9	Social media presence	How often do you post on social media during an average week?	Scale with ranges "times per week."	>20/ 16-20/ 11-15/ 6-10/ 0-5/ 1-3 per month/ less often.	Activity
10	Security routines	How often do you update the units you use to browse social media? 1. Smartphone 2. PC/Mac 3. Tablet	Matrix with check boxes	Every month / every other month / < every other month / Don't know / When asked / Don't have the unit or use it for SoMe	Updating routines
11	Scenario Assessment	Here is a scenario/ answer as you think you would react: You get a message containing a link, do you click it if it comes from … 1. Acquaintance 2. A friend 3. Family 4. Close family	Matrix with alternatives	Yes / No / Maybe	Risk perception and trust
12	Risk Perception	(For Facebook/Instagram users) How do you perceive risk when you conduct the following actions on Facebook/Instagram? 1. Post pictures 2. Post information about your vacation 3. Post pictures of pets with names 4. Share a news item 5. Share a political opinion 6. Share humorous content 7. Participate in public debate	Matrix with scale	Very low / Low / High / Very high	Risk perception when taking an action
13	Risk Perception	Same question as 12, but for Twitter users			
14	Risk Perception	Same question as 12, but for Reddit users			

15	Risk Perception	(For Snapchat users) How do you perceive risk when you conduct the following actions on Snapchat? 1. Post pictures 2. Post information about your vacation 3. Post pictures of pets with names 4. Share humorous content 5. Use Snapmap	Matrix with scale	Very low / Low / High / Very high	Risk perception when taking an action
16	Security routines	Do you use the same password on your social media as on other sites?	Alternatives	I use the same password everywhere / I use the same password everywhere, but use 2FA when possible / I use variations of the same passwords on different sites / I always use different passwords / I always use different passwords and 2FA when it is possible.	Password security
17	Security routines	Have you made any changes to the privacy settings to make your profile less visible?	Alternatives	Yes / No	Exposure
18	Security routines	I limit as much as possible who can see my … 1. Profile on SoMe 2. Contact information 3. Posts 4. Friends and followers 5. SoMe profile visibility in search engines	Matrix with scale	1 – No limitation on visibility/ 2/ 3/ 4 – Strict limitation on visibility/ Don't know.	Exposure
19	Security routines	What information do you have visible to the public on your profile?	Checkboxes	E-mail/ Home town/ Phone no/ pictures of you and family/ political views/ relationship/ family members/ sexual orientation/ I don't know/ I have hidden everything.	Exposure
20	Risk perception	To what degree do you think that your shared information can be abused in an ID theft? 1. Full name 2. Phone number 3. E-mail 4. Social security number 5. Birth date 6. Home address 7. Bank account number 8. Credit card number 9. Health information 10. Accounts and passwords	Matrix with scale	Very small degree/ small/ large/ very large degree	Risk perception on information sharing

21	ID theft	Have you ever had your SoMe accounts hacked? ("Yes"/"Yes, and I …" triggers the remaining questions. "No" sends the respondent to the feedback section)	Alternatives	Yes/ No / Yes, and I am yet to retrieve my account	ID theft
22	ID theft	Do you how your account was hacked?	Multiple choice	Phishing / Password sharing / Hacking / Other / Don't know	Awareness
23	ID theft	(If answered "other") How were you hacked?	Textbox	Free text	Awareness
24	ID theft	What were the consequences, how was your account abused?	Textbox	Free text	Awareness
25	ID theft	What security controls have you taken to secure your SoMe accounts?	Checkboxes	2FA / Changed PW to shorter than 12 characters / Changed PW to 12 char or longer / Periodic PW changes / New log in notifications / Use malware protection / Firewall enabled / Other	Security routines
26	ID theft	How often do you change your password?	Multiple choice	>monthly / every month / every third month / once per 6 months / once every year / <every year	Password security
27	ID theft	(If answered "Other" in Q25) What other security controls have you used?	Textbox	Free text	Security routines
28	ID theft	Have you been hacked again after implementing measures?	Alternatives	Yes / No / Have not implemented any measures	Awareness
29	ID theft	(If answered "No" in Q21) What do you think your social media account can be used for if it is hacked?	Textbox	Free text	Awareness
30	Quality assurance	Feedback on the questionnaire	Textbox	Free text	

Appendix B. Additional Material

Table A1. Overlap between users and services.

		Facebook		**Instagram**		**Twitter**		**Reddit**		**TikTok**		**Snapchat**	
		No	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**	**Yes**
		Count	**Count**	**Count**	**Count**	**Count**	**Count**	**Count**	**Count**	**Count**	**Count**	**Count**	**Count**
Facebook	No	41	0	32	9	20	21	2	39	38	3	22	19
	Yes	0	288	88	200	175	113	138	150	259	29	40	248
Instagram	No	32	88	120	0	86	34	36	84	116	4	41	79
	Yes	9	200	0	209	109	100	104	105	181	28	21	188
Twitter	No	20	175	86	109	195	0	96	99	180	15	41	154
	Yes	21	113	34	100	0	134	44	90	117	17	21	113
Reddit	No	2	138	36	104	96	44	140	0	125	15	23	117
	Yes	39	150	84	105	99	90	0	189	172	17	39	150
TikTok	No	38	259	116	181	180	117	125	172	297	0	59	238
	Yes	3	29	4	28	15	17	15	17	0	32	3	29
Snapchat	No	22	40	41	21	41	21	23	39	59	3	62	0
	Yes	19	248	79	188	154	113	117	150	238	29	0	267

References

1. Alqattan, Z.N. Threats Against Information Privacy and Security in Social Networks: A Review. *Adv. Cyber Secur.* **2020**, *1132*, 358.
2. Gkioulos, V.; Wangen, G.; Katsikas, S.K.; Kavallieratos, G.; Kotzanikolaou, P. Security awareness of the digital natives. *Information* **2017**, *8*, 42. [CrossRef]
3. Studen, L.; Tiberius, V. Social Media, Quo Vadis? Prospective Development and Implications. *Future Internet* **2020**, *12*, 146. [CrossRef]
4. Slovic, P.; Fischhoff, B.; Lichtenstein, S. Facts and fears: Understanding perceived risk. In *Societal risk Assessment*; Springer: Berlin/Heidelberg, Germany, 1980; pp. 181–216.
5. Alhakami, A.S.; Slovic, P. A psychological study of the inverse relationship between perceived risk and perceived benefit. *Risk Anal.* **1994**, *14*, 1085–1096. [CrossRef]
6. Slovic, P.; Finucane, M.L.; Peters, E.; MacGregor, D.G. Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. *Risk Anal.* **2004**, *24*, 311–322. [CrossRef]
7. Loewenstein, G.F.; Weber, E.U.; Hsee, C.K.; Welch, N. Risk as feelings. *Psychol. Bull.* **2001**, *127*, 267. [CrossRef]
8. Gustafsod, P.E. Gender Differences in risk perception: Theoretical and methodological erspectives. *Risk Anal.* **1998**, *18*, 805–811. [CrossRef]
9. Adams, J.G.U. Risk homeostasis and the purpose of safety regulation. *Ergonomics* **1988**, *31*, 407–428. [CrossRef]
10. Kahneman, D. *Thinking, Fast and Slow*; Macmillan: New York, NY, USA, 2011.
11. Finucane, M.L.; Alhakami, A.; Slovic, P.; Johnson, S.M. The affect heuristic in judgments of risks and benefits. *J. Behav. Decis. Mak.* **2000**, *13*, 1–17. [CrossRef]
12. Schaik, P. Risk perceptions of cyber-security and precautionary behaviour. *Comput. Hum. Behav.* **2017**, *75*, 547–559. [CrossRef]
13. Zou, Y.; Roundy, K.; Tamersoy, A.; Shintre, S.; Roturier, J.; Schaub, F. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25 April 2020; pp. 1–15.
14. Gunleifsen, H.; Gkioulos, V.; Wangen, G.; Shalaginov, A.; Kianpour, M.; Abomhara, M. Cybersecurity Awareness and Culture in Rural Norway. In *Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*; University of Plymouth, Centre for Security, Communications and Network Research (CSCAN): Plymouth, UK, 2019; pp. 110–121.
15. Golladay, K.; Holtfreter, K. The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. *Vict. Offenders* **2017**, *12*, 741–760. [CrossRef]
16. Newman, G.R.; McNally, M.M. *Identity Theft Literature Review*; 2005. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.216.6852&rep=rep1&type=pdf (accessed on 25 November 2020).
17. Jagatic, T.; Johnson, N.; Jakobsson, M.; Menczer, F. Social phishing. *Commun. ACM* **2007**, *50*, 94–100. [CrossRef]
18. MILNE, G.R.; ROHM, A.J.; BAHL, S. Consumers' Protection of Online Privacy and Identity. *J. Consum. Aff.* **2004**, *38*, 217–232. [CrossRef]
19. Thomas, K.; Li, F.; Zand, A.; Barrett, J.; Ranieri, J.; Invernizzi, L.; Markov, Y.; Comanescu, O.; Eranti, V.; Moscicki, A.; 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, Dallas, TX, USA, 30 October–3 November 2017; pp. 1421–1434.
20. Nyblom, P.J.B.; Wangen, G.; Kianpour, M.; Østby, G. The Root Causes of Compromised Accounts at the University. In *Proceedings of the 6th International Conference on Information Systems Security and Privacy*; SciTePress: Setúbal, Portugal, 2020.
21. Ur, B.; Wang, Y. A Cross-cultural Framework for Protecting User Privacy in Online Social Media. In *Proceedings of the 22nd International Conference on World Wide Web*; ACM: New York, NY, USA, 2013; pp. 755–762. [CrossRef]
22. Such, J.M.; Criado, N. Multiparty Privacy in Social Media. *Commun. ACM* **2018**, *61*, 74–81. [CrossRef]
23. Van Schaik, P.; Jansen, J.; Onibokun, J.; Camp, J.; Kusev, P. Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Comput. Hum. Behav.* **2018**, *78*, 283–297. [CrossRef]

24. Mitchell, D.; El-Gayar, O. The effect of privacy policies on information sharing behavior on social networks: A Systematic Literature Review. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Hawaii, HI, USA, 7–10 January 2020.
25. Delerue, H.; He, W. A review of social media security risks and mitigation techniques. *J. Syst. Inf. Technol.* **2012**, *14*, 171–180.
26. Gonzalez, D. *Managing Online Risk: Apps, Mobile, and Social Media Security*; Butterworth-Heinemann: Oxford, UK, 2014.
27. Slovic, P. Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. *Risk Anal.* **1999**, *19*, 689–701. [CrossRef]
28. Bickerstaff, K. Risk perception research: socio-cultural perspectives on the public experience of air pollution. *Environ. Int.* **2004**, *30*, 827–840. [CrossRef] [PubMed]
29. Gkioulos, V.; Wangen, G.; Katsikas, S. User Modelling Validation over the Security Awareness of Digital Natives. *Future Internet* **2017**, *9*, 32. [CrossRef]
30. Malmedal, B.; Røislien, H.E. The norwegian cyber security culture. *Norsis Rep.* **2016**. Available online: https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf (accessed on 25 November 2020).
31. Norman, G. Likert scales, levels of measurement and the "laws" of statistics. *Adv. Health Sci. Educ.* **2010**, *15*, 625–632. [CrossRef] [PubMed]
32. Barke, R.P.; Jenkins-Smith, H.; Slovic, P. Risk perceptions of men and women scientists. *Soc. Sci. Q.* **1997**, *78*, 167–176.