Cyber security awareness and culture in rural Norway

Håkon Gunleifsen, PhD candidate

hakon.gunleifsen2@ntnu.no
Student number: 150256

NTNU
Norwegian University of
Science and Technology

IMT 4881 - Specialization Course, 5 ECTS
Department of Information Security and Communication Technology
NTNU Gjøvik , December 14, 2018

Department of Information Security
and Communication Technology
NTNU Gjøvik
Box 191
N-2802 Gjøvik
Norway

Revision history

Version #	Description of change
0	No history

Contents

1 Abstract

Understanding the level of security awareness, the perception, and the culture of users in aspects related to security, is crucial for the development of suitable measures towards their protection and the protection of the utilized infrastructure. This becomes imperative in countries with increased penetration of Information and Communication Technologies (ICT), such as Norway. In this paper, we present the results of a study conducted by NTNU and Eidsiva bredbånd AS, in respect to the security awareness and cyber security culture of Norwegian users of ICT. The study aims to investigate the level of security awareness of Norwegian Internet subscription owners and identify how and if their security awareness can be improved. For that reason, we aim to identify the demographic groups and the characteristics of the security awareness of the Internet users. These attributes have been used to identify the need for knowledge and the cyber security training preferences among different groups of internet users. We have discovered that the level of security awareness is highly subjective and that training programs provided by Internet Service Providers are recommendable.

2 Introduction

Internet access has become an indispensable part of our everyday life, fulfilling the increasing users' desire for connectivity and access to information, social and private networks at any time and place. Amplified by the proliferation of "smart" inexpensive devices, connectivity and online storage are services to which the users become more and more accustomed. Accordingly, the users' security awareness and understanding of potential risks become essential, since they can be exposed to complex types of malicious activity, such as identity theft, blackmailing, active data collection, or defamation. In light of this, it is important that users are aware of both the potential risks and the available countermeasures.

Within this environment, a critical requirement towards a safe and secure information society, is to prepare society for future challenges to personal and professional life, with targeted actions that are aligned with contemporary societal needs. One such challenge is related to our increasing dependency on digital technologies and the corresponding need to improve cyber security awareness. Digitization is a key enabler of growth for the Norwegian state, industry, and society at large. Yet, the security implications at a personal, societal, and corporate level are significant and highly diverse.

Fostering a safe and secure information society is not only a technical challenge. It is a sociotechnical one, which is highly influenced by human factors. As highlighted by earlier studies, the competence, awareness, and risk perception of users, are critical dimensions of cyber security, while the enhanced understanding of the potential impact severity arising from digital vulnerabilities, significantly improves the societal posture against threats at a personal and professional level.

Within this study, we seek to identify critical usage patterns, technologies, user groups, and areas of the private and public sectors, where there is a need for and the possibility of enhancing the cyber security awareness and readiness of the Norwegian society. Accordingly, we aim to study and analyze such sociotechnical attributes as cyber security knowledge, risk assessments and behavioural analysis with a focus on supporting the development of novel intervention actions, educational policies and monitoring methodologies, suitably adjusted to the requirements and characteristics of the Norwegian society.

Accordingly, the aim of our long-term study is to investigate the security awareness of Norwegian internet users, with respect to various indicators such as age, gender, residence, educational background and work environment. Consequently, we will seek to identify, propose, and implement suitable countermeasures, in order to promote a more secure networking culture from the users' perspective. This paper presents the results from a survey, conducted for the purpose of establishing and evaluating the data collection and collaboration tools between NTNU and Eidsiva bredbånd AS. In addition, we seek to create a training program for their internet users. For that reason an understanding of their skills and their security awareness is crucial. Our results outline generic properties of the sample, and categorical differences within the delimited focus areas. The questions have been targeted to a subset of focus areas that provide crucial initial inputs towards further evaluation, with a sample size that supports sufficient confidence on the results.

This paper is structured as follows: This chapter introduces security awareness and our main objective with this paper, while the next chapter presents the problem description and some of our hypotheses. This is followed by chapter 4 that gives a short literature review of the related work and chapter 5 presents our research method and our survey sample. Chapter 6 is the main part of this paper, where we analyze the results of the survey and discuss our hypotheses. Chapter 7 concludes this paper.

3 Problem description and Objectives

We aim to perform a study of the Norwegian cyber security culture with particular focus on the home environment. Previous studies show (Chapter: 4) that there is a need for cyber security training within home environments in particular. The Norwegian center for cyber security (NorSIS) has emphasized the need for enhanced and focused cyber security training in order to raise the general level of security awareness in Norway [13],[14]. They claim that Norwegian Internet Service Providers among others, have a role in the society for providing the training necessary to increase the general security awareness. The Norwegian Internet Service Provider, Eidsiva bredbånd, aims to pursue this challenge in collaboration with the Norwegian University of Science and Technology (NTNU). Accordingly, in this study we seek to explore the following:

- NorSIS state that cyber security awareness is low in Norway and that more knowledge is needed [14]. Why is it so and does this also apply to the Internet subscription owners of Eidsiva bredbånd?
- Which are the common attributes among those who do not have the required security awareness level? Can we identify groups of people that have different needs for training?
- How can Eidsiva bredbånd provide cyber security training for their customers?

In order to provide cyber security training facilities, Eidsiva bredbånd aims to identify the content and the training method that would be optimal for the different groups of subscribers. For that reason, it is necessary to identify the security awareness attributes of their customers. The five-steps ladder model of Khan et al [10] is followed for measuring the level of information security awareness. For comparison reasons, we simplified the model to include measuring of interest, knowledge, risk evaluation and behavioural analysis, similar to the NorSIS report. Therefore, in addition to the standard security awareness measurements, we introduced a set of new hypotheses related to training and demographic attributes. Hypotheses:

- Some believe that people in rural areas are less concerned about their home security. For example: In the rural areas, some people choose not to lock their door on a daily basis, because they generally feel safe. We wanted to transfer this hypothesis to the cyber security domain and asked: "Are people in the rural areas less concerned about their cyber security than users in other areas?"
- Do big companies have more resources for cyber security training than smaller companies? Is this reflected in the cyber security awareness of the employees in their home environment?
- If men are more willing to take risks in life in general, is this also transferable to cyber security?
- How does age affect the level of cyber security awareness?

- Are more educated people more security aware and more positive to cyber security training?
- How does the employment sectors, such as the ICT employment sector, affect the security awareness of the users in their home environment?

We seek to project the aforementioned hypotheses towards demographic attributes, such as: Gender, age, living area, education, and employment sector. Hence, these attributes combined with general security awareness studies and training studies allow us to perform:

- Analysis of the current security awareness level across the identified domains, indicators, and groups.
- Identification of suitable indicators, within the Norwegian society, which can allow the fine-grained categorization of the public, and the definition of targeted security awareness programs.

4 Related work

Kruger et al [11] aimed to create a model that measured the effectiveness of security awareness programs in gold mines based on their general stance, knowledge and behavioural patterns. This and other organizational studies [12], [17] have shown that collective employment participation and education is imported factor in order to increase general security awareness. However, the NorSIS report from 2018 [14] states that cyber security awareness is not only an organizational culture, but it is a national and global culture. The last Global Information Technology Report [5], published by the World Economic Forum, shows that Norway is among the top 10 countries in respect of both usages of digital service of and digital readiness in respect of capitalizing on digital platforms. Hence, studies of cyber security cultures in Norway are highly relevant due to their digital evolution. However, the NorSIS report has also shown how the Norwegian cyber security culture has not evolved for the last years and pinpoint that education is national responsibility for both internet service providers, companies and the government. Together with Talib et al [22], they point out that cyber security cannot be archived by technical means alone. Their studies have shown that the majority of cyber security training exist at home and at work. Also, that training at work is transferable to the home environment. Cyber security awareness in home environments, and for those who do not work, is not a research topic that has gained much attention. Hence, we aim to identify the attributes to different groups of people in home environments. One of these groups is age. It is not found any relevant study of the security awareness for the older generations only. However, studies on the youngest generations, the digital natives, are more extensive.

Prensky [19] writes that digital natives, the people who have been exposed to digital technology since birth have a different view on digital technology than older generations. Studies have shown [8] that digital natives tend to have increased confidence in the daily use of technology, but it also leads them to neglect cyber security related matters. Correspondingly, a Slovenian study [15],[16] showed a low awareness of security threats and security measures among digital natives. The users tend to prioritize access to services and usability over the enforcement of security measures and digital natives are in fact more willing to accept risks despite their knowledge about cyber security. Ariu et al [4] confirmed these studies and shows that the perception of a higher cyber security knowledge among digital natives is wrong and that they are unaware of the risk arising from their behaviour.

From a threat perspective, people tend to alter their behaviour based on the amount of risk they perceive. End-users that believe they are under a high threat, alter their behaviour to counter the consequences. However, when end-users believe they are not at risk, they become less cautious. End-users tend to take more risk and care less about security when they have installed security products or when they believe they are using their digital devices in a secure network domain [24]. This complicates the security awareness and results in a paradoxical situation where technical security solutions can degrade the security awareness of end-users [23]. This is also reflected in business organizations where ICT technical staff considers end-user incapable of handling security-related tasks. This results in information sharing from ICT staff to end-users on a need-to-know basis, where the staff upheld the paradoxical situation and hinders the security awareness among end-users [8].

The studies [24],[4],[8] show that the security awareness, in general, is low and that general cyber security education is needed for end-users, including both for digital natives and the older generations. However, the studies do not conclude in consolidating a concrete relation between digital natives and security awareness, something that indicates that other attributes such as culture and background are also likely to have an impact on security awareness.

The educational need suggested in the aforementioned research is a challenge for a nation with many governmental departments, companies with different security focus and a wide range of service providers. NorSIS discovered that security is not primarily taught from security specialists or in school, but end-users mostly learn from each other. Internet Service Providers, such as Eidsiva bredbånd can contribute to cyber security education as well as protecting the end-users through their infrastructure. However, based on the studies from NorSIS, the education is suggested to be targeted. For that reason, a comprehensive study of security awareness is needed to find the educational need by demographics and cultural differences in order to identify and deploy targeted solutions in both a national context and for local Internet Service Providers such as Eidsiva bredbånd.

5 Methodology

This section has the following structure: the first sub-section addresses the choice of data collection method and instrument, followed by the sample description, and a brief overview of the statistical methods used for data analysis.

5.1 Data collection, Sample, and Instrument

The data collection aimed to explore the security awareness of the persons in the rural areas of Norway and compare their perceptions to other groups citizens. Hence, this article explores the security awareness of the people living in the rural areas of Norway, primarily Hedmark, Akershus, and Oppland counties. The target group was reached using the customer lists of the biggest Internet Service Provider in the region, Eidsiva bredbbånd. We found the online questionnaire to be the best option for data gathering as it reaches a broad audience, is easily distributed, and provides a strong level of anonymity. The target group has in common that they are subscribers to Eidsiva, and being so, are very likely located in the rural side of Norway. We define rural as being outside the big cities, such as Oslo, Bergen, Trondheim, and Stavanger. Belonging, as the area of living, is also a mandatory categorical variable in the questionnaire to clarify this issue for all respondents. However, the term rural is relative to the area of living. Furthermore, all subscribers must be above 18. The survey was distributed by the Eidsiva communications department to a selection of approximately 10000 customers, and was live in 10 days in October 2018. With a total of 945 respondents, the survey had a little less than 9,5% response rate.

The survey had 71 questions that investigated security awareness aspects within the areas outlined in the problem description (Chapter: 3). Hence, the questionnaire was designed to measure security awareness within specific key knowledge areas of cyber security; Stance, Knowledge, Risk evaluation, Trust, Training and Behavioural patterns. As for the level of measurement, the questionnaire had category, ordinal, and continuous type questions. Category type questions are used here mainly for demographics, while the main bulk of the questionnaire was designed using several mandatory scale and ranking questions. The categorical variables we surveyed were: Gender, Age, Belonging, Education, Work, and Company size.

5.2 Analysis

We applied a variety of statistical data analysis methods specified in the results, and the IBM SPSS software [21] for the statistical analysis. A summary of the statistical tests used in this research is as follows:
For *Descriptive analysis* we have considered distributions including range and standard deviation. On continuous type questions, we applied measures of central tendency mean, median and mode. We also conducted *Univariate* analysis of individual issues, and *Bivariate* analysis for pairs of questions, such as a category and a continuous question, to see how they compare and interact. However, we have restricted the use of mean and standard deviation for Likert-type questions and ordinal data where there was not defined a

clear scale of measurement between the alternatives, as the collected data will seldom satisfy the requirements of normality. We have, therefore, analyzed the median together with an analysis of range, minimum and maximum values, and variance. This study also analyses the distributions of the answers, for example, if they are normal, uniform, binomial, or similar. *Crosstabulation* was applied to analyze the association between two category type questions, such as "Company Size" and "Expertise." We have used Pearson two-tailed *Correlation test* to reveal relationships between pairs of variables as this test does not assume normality in the sample.

An attribute of these tests, such as for the Pearson two-tailed *Correlation test*, is the probability value (p-value), that refers to the mean difference between two compared groups and the probability of a correlation. We refer to this value during our analysis of the result to show the level of difference between the demographic groups for the questions. A p-value below 0,005 is considered as a significant deviation. Another term we refer to during our analysis is *Skewness*. We refer to skewness as a measurement of the asymmetry from the normal distribution.

For each group of questions, the procedure was as follows: Firstly, we analyzed the results as-is (univariate), where we use the term "face-value" for this data. Secondly, we ran a bivariate analysis to test our hypothesis regarding differences in results between groups. Furthermore, we ran ANOVA tests where they were applicable to test for statistically significant differences between categories and to test the hypothesis.

6 The results of the study

This chapter analyzes and discusses each question in the survey. As mentioned in the Introduction (Chapter: 2,3), the questions were divided into seven categories that represent the sections in this chapter. For each section, we analyze the data and present the distribution of the replies per question - the face-value data. Additionally, we ran the correlation tests towards the demographic attributes and present the most significant findings. The key findings are summarized per section for each of the seven categories. First, we present the categorizations questions in Section 6.1, where the sample data of gender, age, living area, education, working sector and company size is discussed. This is followed by four sections of security awareness analysis where their general stance towards cyber security (6.2), their knowledge (6.3), their risk evaluations (6.3) and their trust (6.4) in service providers and authorities are discussed. Section 6.6 analyzes the training preferences among the users, while Section 6.7 compare their self-evaluated skills in knowledge and risk-evaluations with their actions and behaviour online.

6.1 Demographics

We surveyed gender, age, living area, education, employment sector, and the number of employees in their company. Out of the 945 respondents we got 715 (75.7%) males and 230 female (24,3%) responses. Based on the subscription owners of Eidsiva bredbånd, this sample corresponds to their general base of customers. Their average age were relatively high, where 59% of the users were above the age of 56 years (Figure: 1). It is reported that the average age of all customers of Eidsiva bredbånd is years 53,7 years and that they have 63.000 customers. The main reason for this old average age is according to an Eidsiva interview that the subscription owner is often a parent or a person that belongs to the oldest generation in a household that most commonly is the subscription owner fixed-line internet connections subscriptions. This age does not represent the general population. However, according to the initial description of surveying subscription owners, this represents a good sample of subscription owners. Also, there is a limited number of surveys that particularly focus on the security awareness of the elder generation. The reason for the slight age skewness of more elderly people compared to the general customer base of Eidsiva bredbånd in the sample is not identified. It is also identified as a significant skewness in gender. However, this number also represents the general customer base of Eidsiva bredbånd. It is not known why it is primarily the man in the house that signs up as the subscription owner of the internet connection of the households.

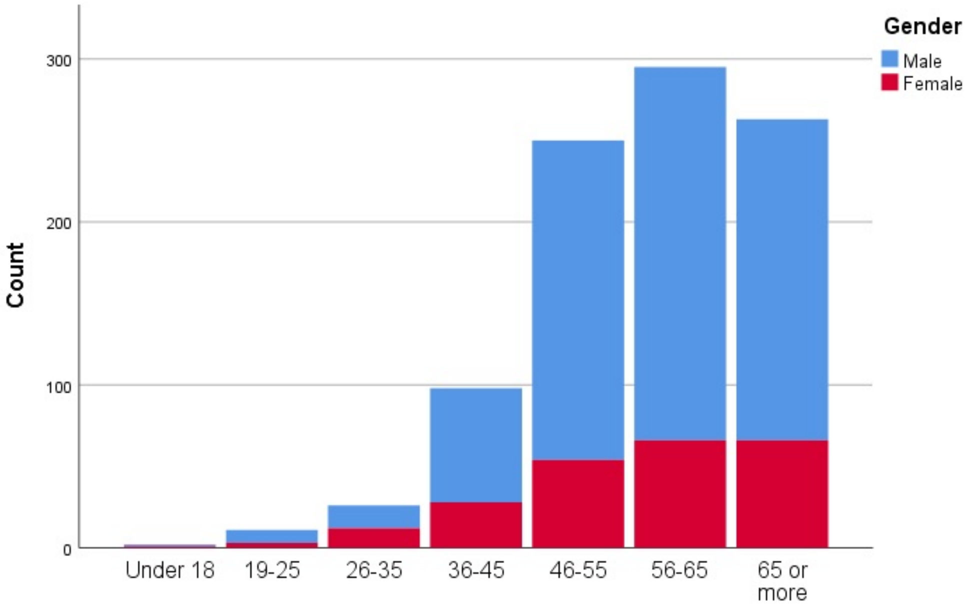


Figure 1: Age and gender distribution in the sample

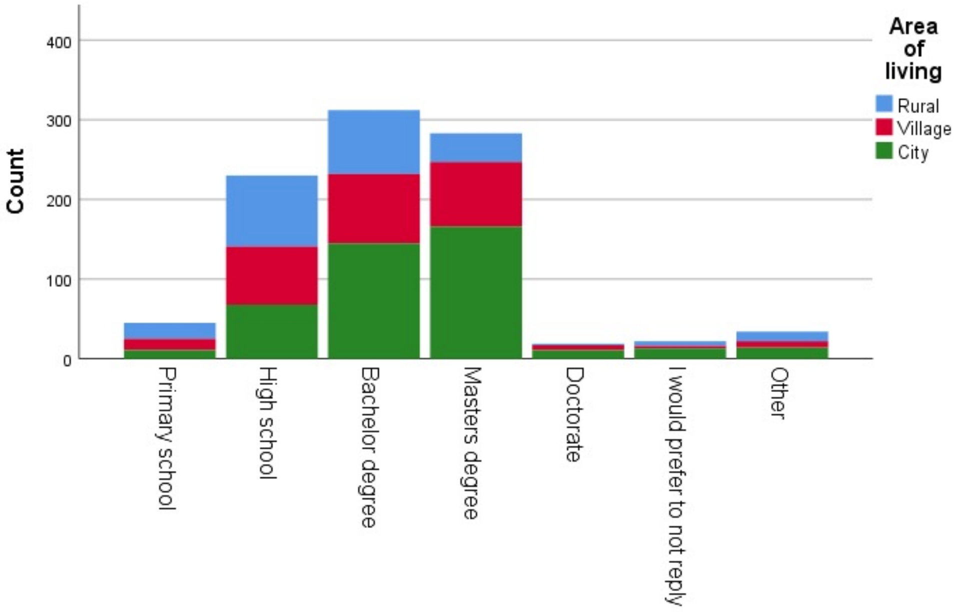


Figure 2: Strong correlation between educational level and the living area

Another set of categorical attributes we used were educational level and area of living. The main area of Hedmark and Oppland has a population of around 400.000 [3] inhabitants where The 6 largest cities have populations between 10.000 and 30.000. We let the users define if they were living in a rural area, a village or a city, that is assumed to be considered relative to the surrounding population. One of the objectives of the survey was to identify if there were any differences in security awareness between people living on the countryside/rural areas versus the people in the city. 45,3% users responded that they were living in the city, 28,8% in a village and 25,9% were living in rural areas. However, the results showed that there was a strong correlation between the educational level and the area of living (Figure: 2). This makes it difficult to identify if a difference in security awareness based on living area is due to their educational level or their living area.

64,0% of the respondents had a higher education from a college or a university, that is much more than there average population in Norway (33,4%) [2]. It is not known if educated people tend to respond more willingly to surveys or if subscriptions owners of fixed-line internet connections are more educated in general.

The last two demographic attributes we defined were the employment sector (Figure: 3) and the number of employees in their workplace (Figure: 4). We aimed to identify if there was any employment sector in Norway that was better to give cyber security training than others. Also, it is relevant to measure if there is a connection between the number of employees and their level of security awareness. It is likely to believe that big companies have more resources to perform security awareness training than small companies.

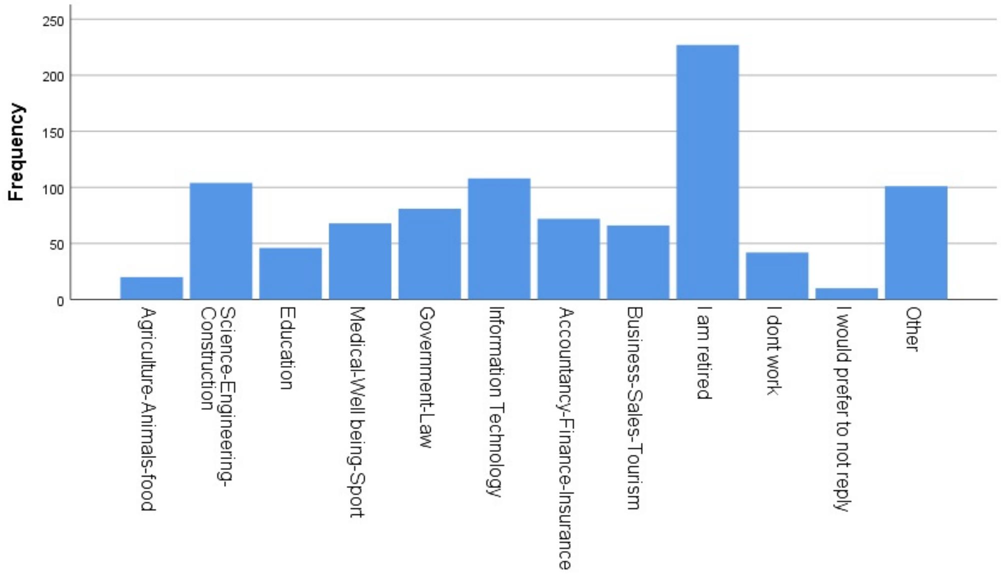


Figure 3: Distribution of employment sector

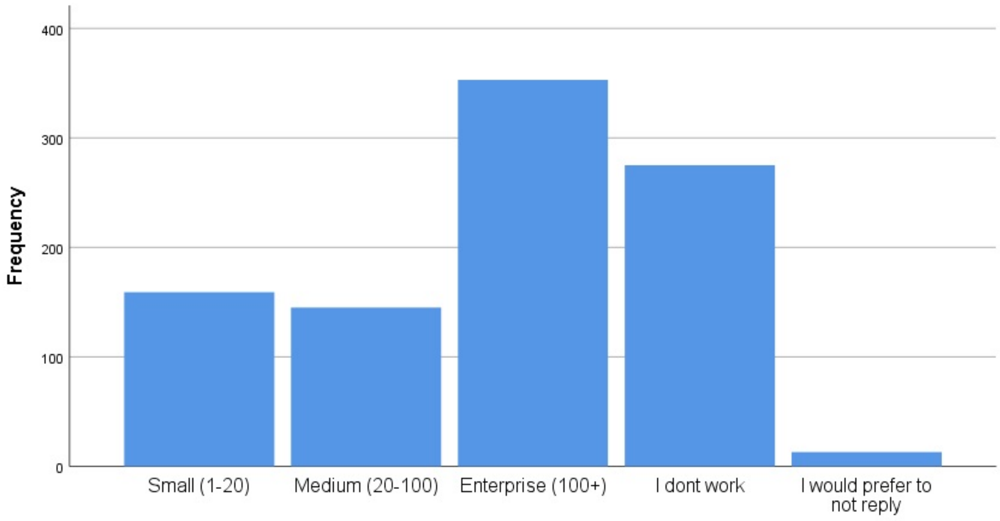


Figure 4: Distribution of number of employees at the workplace

6.2 The general stance towards Information Technology

An important factor when people are asked about their security awareness is their relation to technology in general. If people are not interested in ICT or computers at all, it is a high probability of a generally negative response or simply rejecting the survey. An important factor for verifying the quality of the survey is, therefore, to measure the general interest among the users and compare the level of interest to other sources.

6.2.1 The general interest in Information Technology

The users were asked: "What is your interest in Information Technology", and rated that on a scale of 5 categories. The received results had a slight skewness to them, where the general stance was that they were over average interested. 40,0% of the respondents answered over average or very interested in ICT, while about 17,1% claimed to have little or no interest (Figure: 5). The NorSiS report from 2018 [13] confirmed that interest affects attitude, skills, knowledge and awareness. The level of interest is therefore affecting all the other answers. Also, this is a strong indicator of whether our sample is a representative selection, comparing to other recent studies. The NorSIS report from 2018 also claims that a national level of interest indicates that 25% has little or no interest, while 48% has over average or very high interest in ICT. This is slightly different than our result, but our sample is different since we, in particular, have asked internet subscription owners of households connected to with fixed internet lines such as cable, xDSL or fibre, that tend to be elderly men.

There is a strong variation (p=0.000) between general interest, gender and age. Men tend to be more interested in ICT than women. (Figure: 5). This is also confirmed by the NorSIS report where 63% of the men and 35% of the women are interested or very interested in ICT. In our results 46,1% of the men and 20,8% of the women er over average or very interested in ICT. More interestingly, there is also a significant variation in the correlation to age, but it is not a clear indication of whether increasing age is fully linear to decreasing interest. The age groups of above 46 years have less interest in technology than the younger people. For people above the age of 46, the responses are similar, averagely normal distributed, while people below 46 tend to have a more interest towards ICT. However, since our sample is mostly elderly men, this clearly explains the difference in our sample compared to the NorSIS survey. That means that the face-value of our data is not representative of the general population, but the distributions within the demographic groups are still expected to be good enough to show significant variations and correlations.

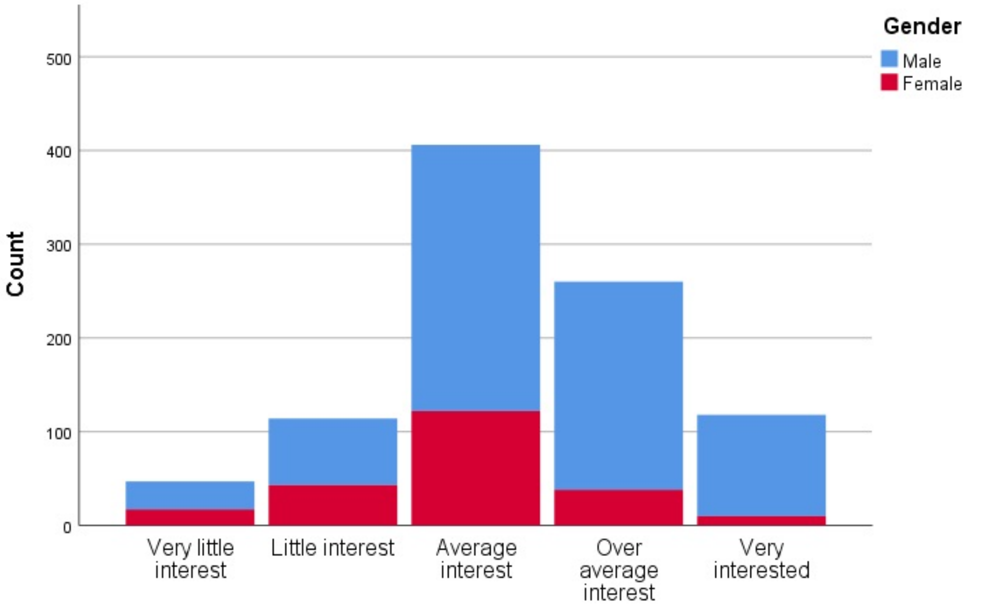


Figure 5: Degree of interest in Information Technology by gender

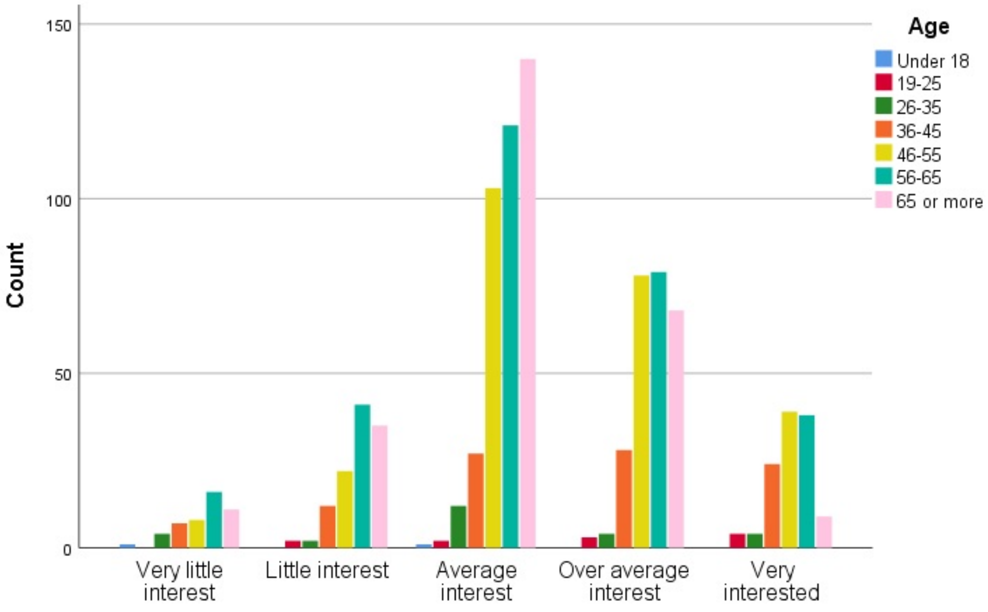


Figure 6: Degree of interest in Information Technology by age

A high level of technology interest also has a connection towards both educational level of bachelors or above and centralized living areas. (Figure: 7,8). Meaning that educated people and people in the city are more interested in ICT than others.

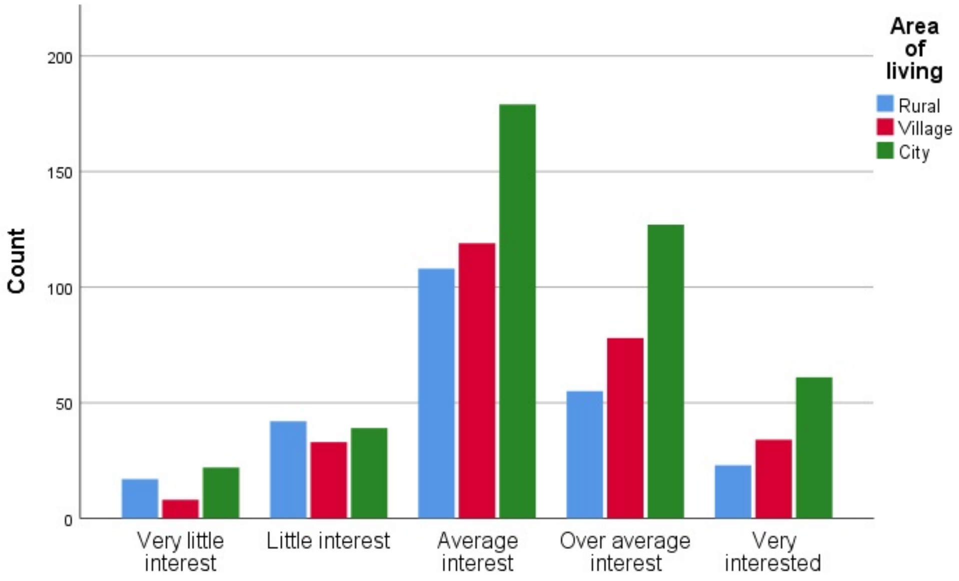


Figure 7: Degree of technology interest by area of living

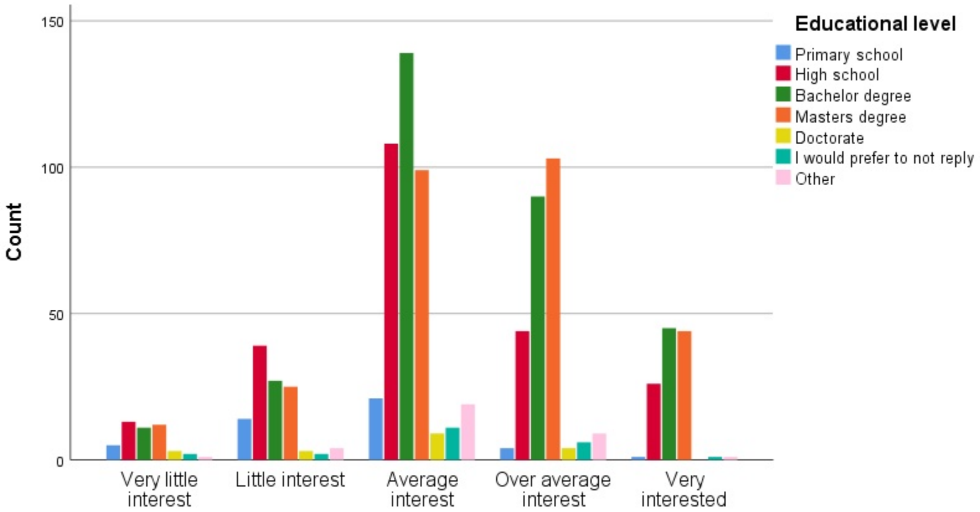


Figure 8: Degree of technology interest by educational level

Apart from the working sector of ICT there is not found any other correlations to the interest of ICT.

However, being interested does not necessarily correspond with the level of how positive they are to cyber security. Interestingly, the number of people that is positive to cyber security is much higher than the average interest. 78,7% did partly agree or agree to be positive towards cyber security (Figure: 9).

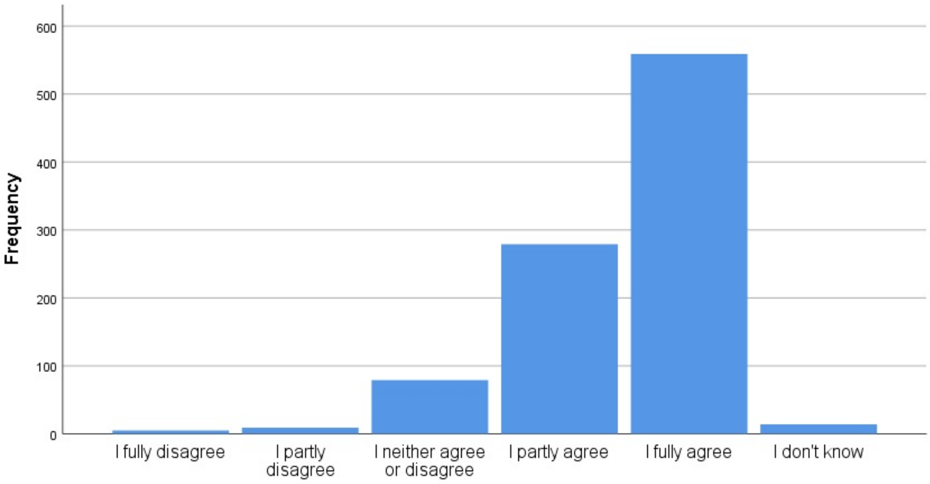


Figure 9: The level of how much the users agreed to be positive towards cyber security

As expected, the level of being positive also correlates with interest where we see similar distributions of gender, living area and education. Hence, they are more positive in the cities than in rural areas. However, the age seems to correlate much more with the face-value data. That means that the level of being positive toward cyber security is independent of age, where all generations seem to be generally positive to cyber security. It is also noticed that we did not find any correlation between the employment sector and being positive to cyber security. For example, the people who work with ICT does not have significantly higher interest for it ($p > 0.005$) than the rest of the participants in the survey. This clearly shows how subjective the question is.

6.2.2 Tolerance of security measures

In order to make a system, computer, network or a mobile phone safe, security measures such as enforced password changes, antivirus and service restrictions are elements that protect the users. Some of these measures can be perceived as problematic and sometimes also unnecessarily restrictive. Security measures most frequently intended to protect the users. However, if the users are not aware of or don't understand why the security measure is there, then it can be perceived as an obstacle. We asked the participants how much they agreed in the statement: "Security measures reduce user friendliness". 23,8% fully or partly disagreed to that, while 41,7% partly or fully agreed.

We did not find any variations between the employment sector or the number of employees in companies. Neither between gender, age or educational level. However, the area of living attributes showed that the people in the city (49,3%) partly or fully disagreed to that, while 24,0% or the people in the rural area had a similar opinion (Figure: 10). As seen previously, living area correlated with educational level, but for this question, we see this variation that is not correlating with the other demographic attributes.

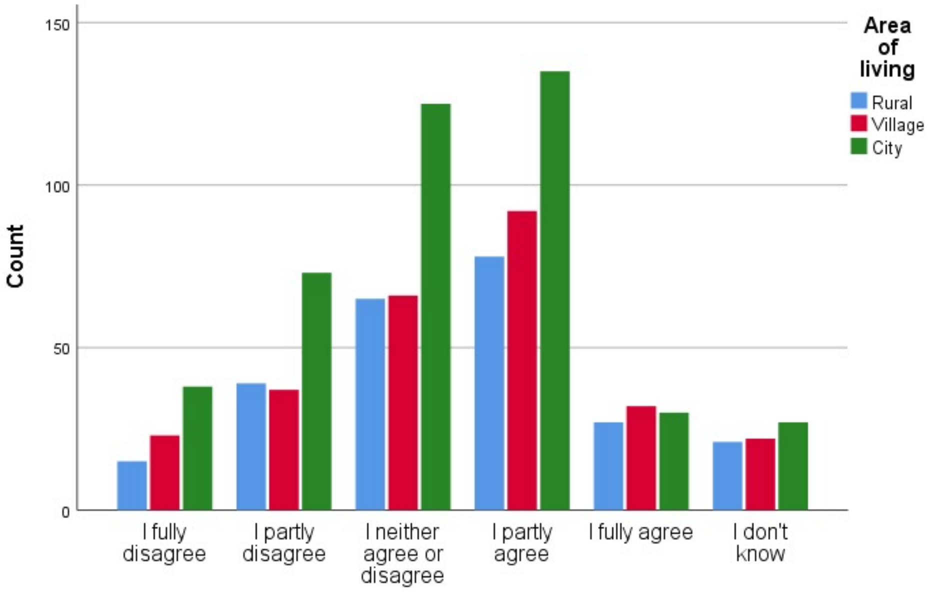


Figure 10: The level of agreement to the statement that "Security measures reduce user friendliness measurement" distributed by area of living

Between the questions, there is a clear indication, that the group of users that is interested, is also the users that have the least tolerance for bad friendliness in security measures. Correspondingly the people that self-evaluate their knowledge to be high, have a low tolerance for bad friendliness in security measures. The knowledge is discussed in the next section (Section: 6.3).

6.2.3 Summary of the general stance towards cyber security

The sample is over-represented by elderly men that affects the total result. 40,0% of the respondents claim to be over average interested in ICT while 78,7% did partly agree or agreed to be positive towards cyber security. 23,8% did fully or partly disagree to; "Security measures reduce user friendliness". Among the group of interested and positive people, 43,6% partly or fully agreed, while 29,9% partly agreed or disagreed to the statement that security measures reduce user friendliness. We know that positive and interested people are more security aware, but a significant group of these people are also negative to the friendliness for the security measures. If being negative to the friendliness of the security measures also includes that they do not see the need or if it is just annoying, then this can influence the respect for the security measures and potentially also result in users avoid using it. Another interesting observation is that the NorSIS sample had a higher interest for ICT than our sample, while our sample was more positive to cyber security than the NoRSIS sample.

6.3 Cyber security knowledge

In NorSIS report [14], they write that: "The Norwegian society becomes increasingly dependent on technology, where individuals are given more responsibility of handling basic skills with Information Technology." They further write that; "It is expected from the society and the government that people attain knowledge of how to use it without necessarily been given the opportunity or resources for it. This can leave the individuals to feel forced to use technology they don't want to use." However, it definitely means that it is the responsibility of individuals to take actions of gaining knowledge. Here, cultures and subcultures potentially can define how people are taught. It is of our particular interest to observe if the customer base of Eidsiva bredbånd has any different level of knowledge, how they have obtained it and if there are any groups within the region that differentiates themselves.

6.3.1 Self-evaluation of cyber security knowledge

We asked the subscribers how they evaluated their own knowledge in cyber security. The background of this question was to determine if there is a connection between knowledge and awareness. This perception of knowledge question is a baseline for later evaluations, where it is also seen in correlation with knowledge about basic security awareness principles. Another aspect of this question is: If not having the knowledge, makes a person more precocious and therefore also more security aware. We categorized the responses in three categories by rating their knowledge to be less, the same or more than an average person.

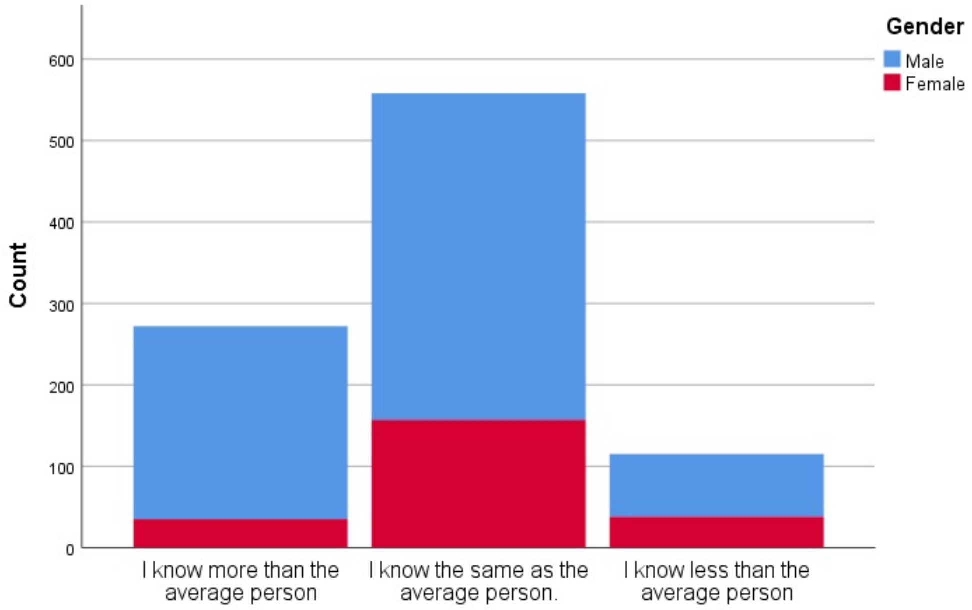


Figure 11: Self-evaluation of cyber security knowledge by gender

The results (Figure: 11) shows that most of the users consider themselves average or above in having knowledge, according to a slightly skewed distribution, where 28,8% claimed to know more than an average person and 12,2% knew less the average person. This is a slightly better result than the average population, where 24% claimed to know more and 18% claimed to know less than an average person. However, this questions if the perception of knowledge is higher among the population than it really is. This is because a true normal distributed result would be fully equally distributed. But, it is possible that internet subscription owner generally has a higher level of knowledge than the rest of the household or the rest of the population.

In respect of the correlations to the demographic attributes, all attributes had strong deviations from the normal distribution (p > 0,005). Figure 11 shows that men clearly consider themselves to have more knowledge them women, that also can explain the deviation from the NorSIS report.

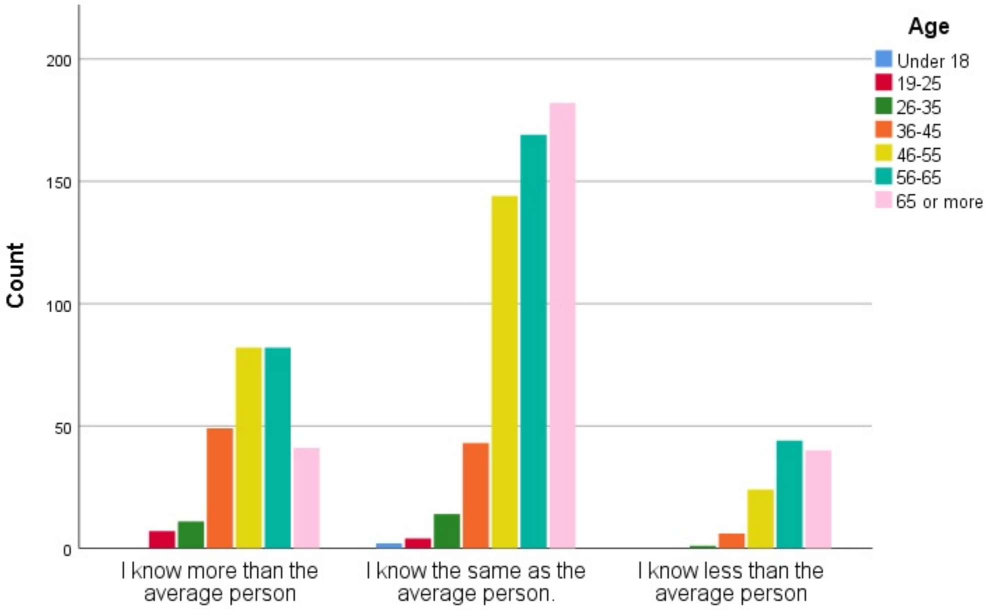


Figure 12: Self-evaluation of cyber security knowledge by age

The age group also have deviations from the normal distribution, where young people score themselves relatively higher than elderly. However, this result was different than excepted, because the deviation for the NorSIS report cannot be explained. Since the sample of Eidsiva bredbånd is mostly elderly people, it was excepted that they would have scored themselves lower. However, all different groups of age, scored themselves better than the national population of Norway.

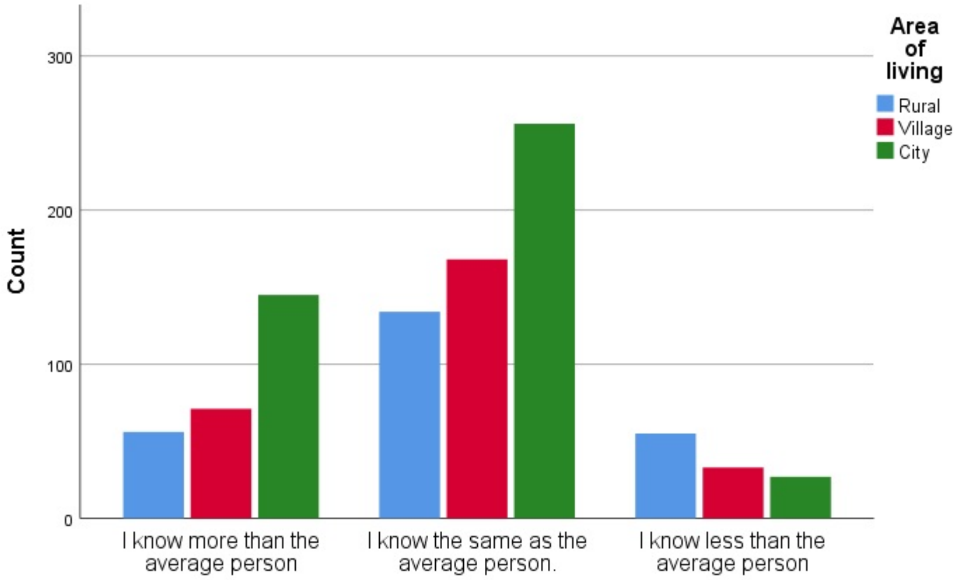


Figure 13: Self-evaluation of cyber security knowledge by living area

There is also statistically significant differences between the educational groups and the living area groups. Both people in the city and educated people consider themselves to know more (Figure: 13, 14).

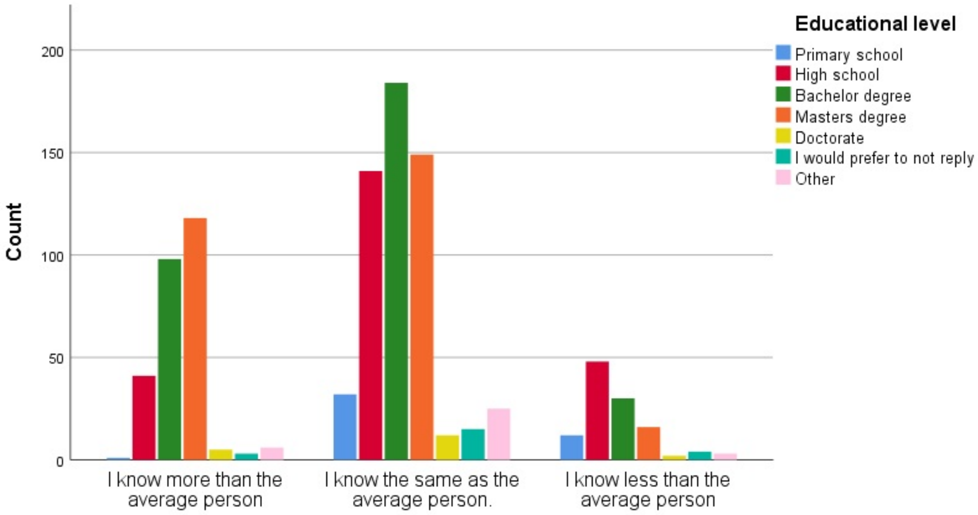


Figure 14: Self-evaluation of cyber security knowledge by educational level

The one-way ANOVA tests showed that retired people and the users working with ICT deviate the most from the normal distribution in respect of their knowledge evaluation. Respectively retired people consider themselves to know less and ICT people more (Figure: 15). This is also seen when evaluating the knowledge level based on company size (Figure: 16). Here, we also see a slight indication, that the users in big companies generally rate themselves to have a higher level of knowledge than the other groups.

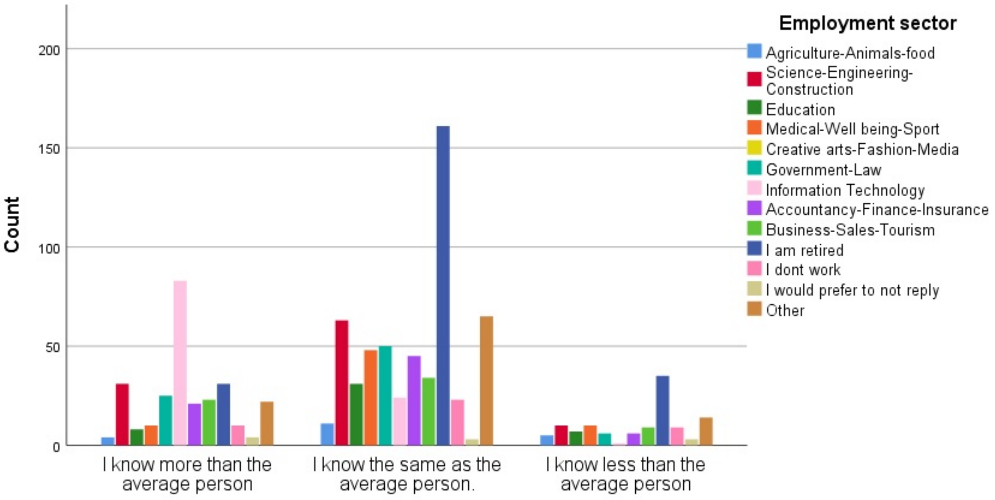


Figure 15: Self-evaluation of cyber security knowledge by employment sector

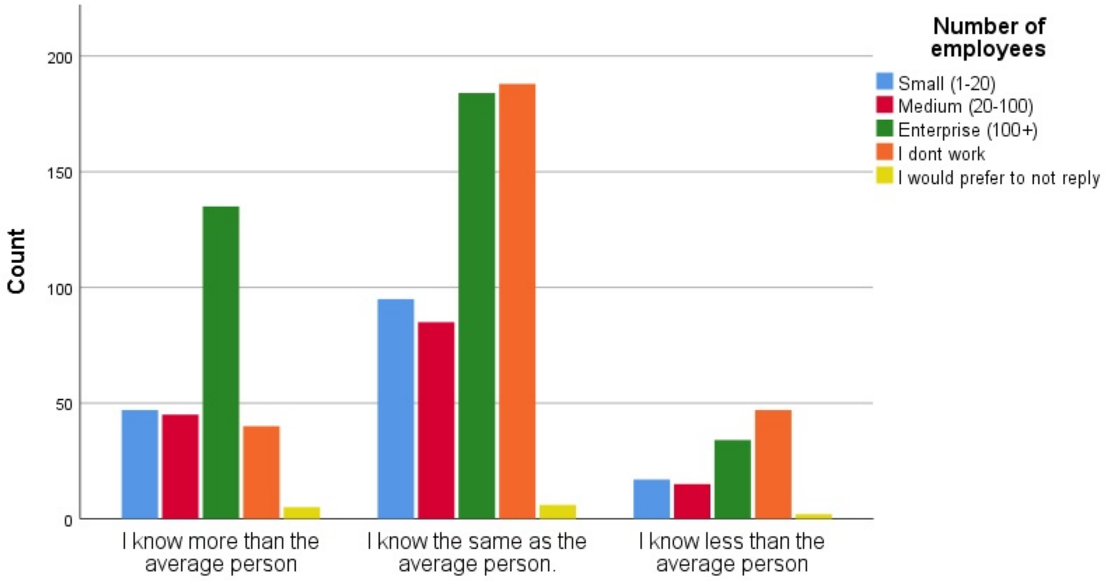


Figure 16: Self-evaluation of cyber security knowledge by number of employees

6.3.2 Scaling knowledge

Asking the users about their knowledge level also gives two different normalization graphs, depending on asking them; if they consider themselves to know more than others or based on a standalone scale. On their own scale (Figure: 17), 44% give themselves the highest score of fully agree to that they know what cyber security technology is, while 28,8% claims to know more than the average population (Section: 6.3.1). This confirms our assumption mentioned earlier and the subjectiveness of the questions. This shows that there is a difference in knowing the existence of something versus knowing how to use it. The replies could potentially indicate that the users meant they have heard about the term, but that they do not know that they don't know. This we do not know. An analogy to that is if we asked the people: "If they knew what is a car was", then most people will probably say "Yes". However, there is a difference in knowing what a car is, versus knowing how to drive it, repair it or how to avoid accidents with it.

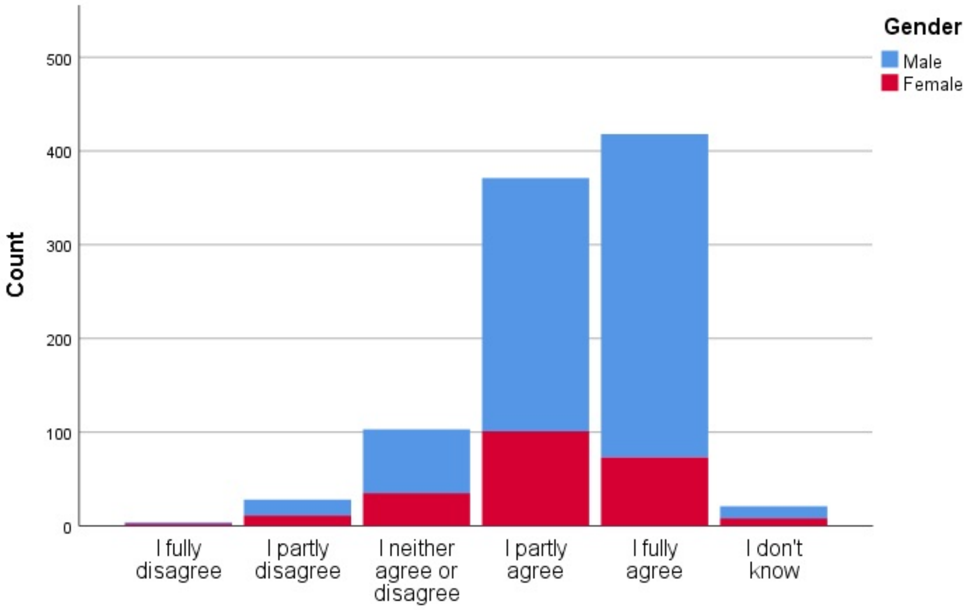


Figure 17: Self-evaluation of knowledge - The level of agreement in knowing what cyber security is, categorized by men and women

6.3.3 Feeling informed about threats

We asked the people how well they felt about being informed about online threats. 90,9% partly agreed or fully agreed to feel well informed about online threats (Figure: 18). In the light of demographic correlations, there seem to be no deviations within the distribution in respect of how informed the users felt about online threats. Surprisingly, the retired people responded to be almost equally informed about online threats as the people working in big companies (Figure: 19). The question is obviously highly subjective because it is a self-evaluation, but it questions the scale people are using when answering this question. Also, it is possible that is is a gap between what the national security authorities consider to be "informed" and what the general population thinks.

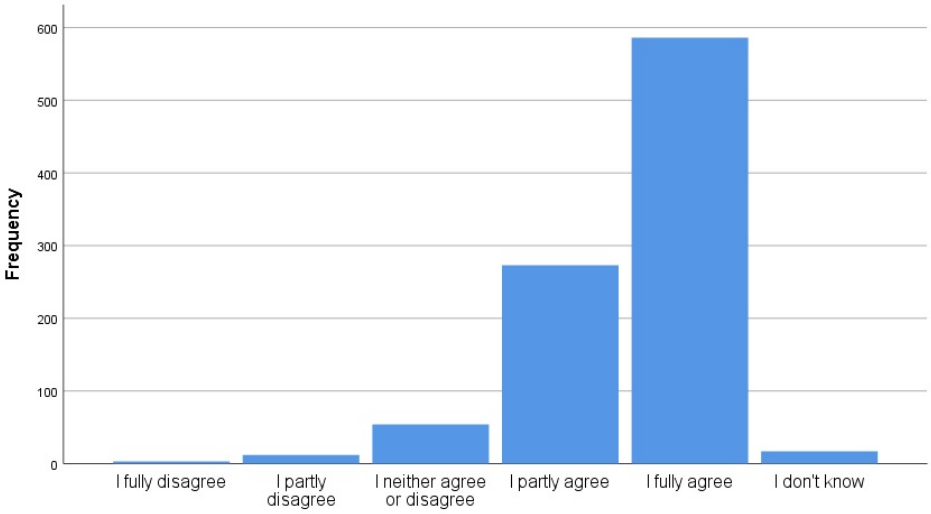


Figure 18: How much the users agreed in feeling informed about online threats

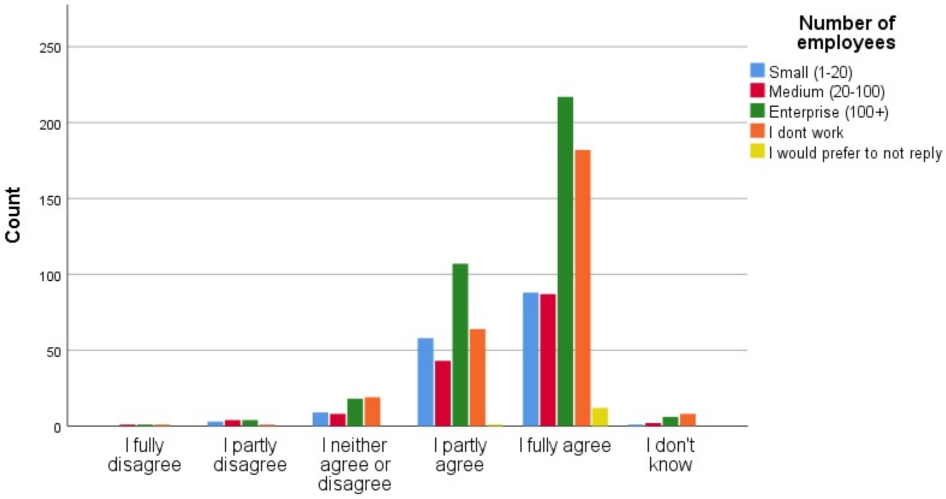


Figure 19: How much the users agreed in feeling informed about online threats, related to the number of employees

6.3.4 Awareness of cyber security regulations

This question intends to baseline the users' perception of knowledge towards a concrete question about cyber security question. Ahead of the implementation of GDPR [6], GDPR got attention in both industry and media during the first part of 2018 in Norway. It is therefore excepted that many people associate a regulation with i.e. GDPR. The question also measures if people are aware of their rights and also if they are aware if they are breaking the law. Reports about a high level of online harassment [1], compared to non-online harassment, indicate that online harassment is generally considered easier to "perform". The studies from Medietilsynet [1] indicate many reasons for this, but the lack of knowledge about the regulations is one hypothesis of a contributing factor. Hence, we asked the user if they were aware of any cyber security regulation. 65% of the users answered "Yes". The result indicates as mentioned earlier that perception of knowledge is relative. However, even if 90,1% claims to be aware of online threats and only 65% is aware of any security regulations, it is not possible to state that their perception of knowledge is higher than the average knowledge level.

With respect to the demographic attributes, we found a correlation to gender and to the area of living, but the other groups also had significant variations. It registered that men claim to have a higher level of knowledge, but they scored equally to women in measuring if they knew about any security regulations. The different age groups were similarly distributed, but the age group above 65 years were less aware than the others. Only 53,6% of them knew about any regulations compared to the other groups where 70-80% of all the other age groups answered "Yes" (Figure: 20). One hypothesis is that this is related to the working environment and, potentially, also the implementation of GDPR in many companies. The connection to companies is confirmed by seeing the correlation to employment sector, where the people that don't work and the retired people are less aware of any regulations (Figure: 21). For those who do work, there is a clear difference in the level of knowledge for those who work in a company with many employees. However, also the smallest companies seem to have significantly more knowledge about regulations than medium companies and for those who are not (Figure: 22).

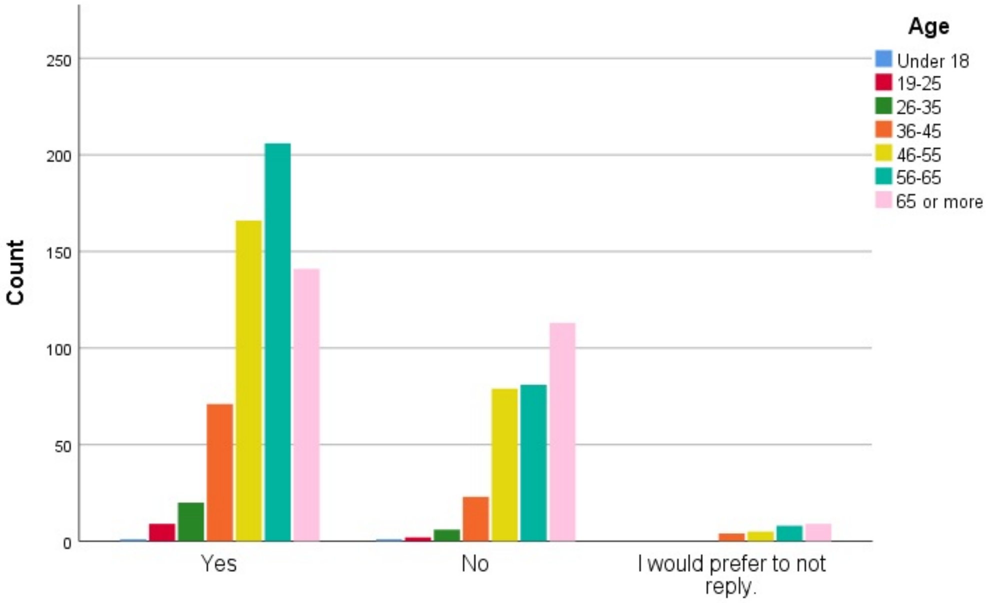


Figure 20: If the users have knowledge about cyber security regulations by age distribution

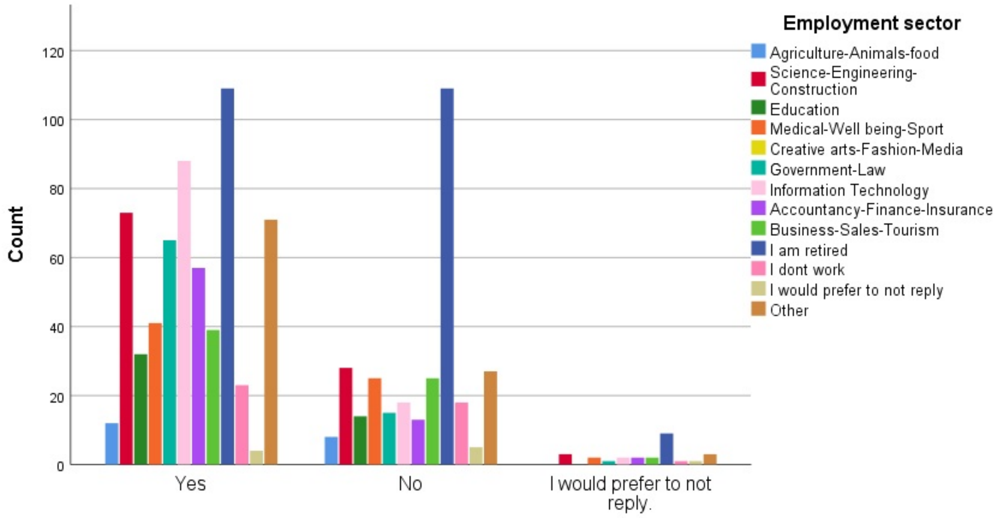


Figure 21: If the users have knowledge about cyber security regulations by employment sector

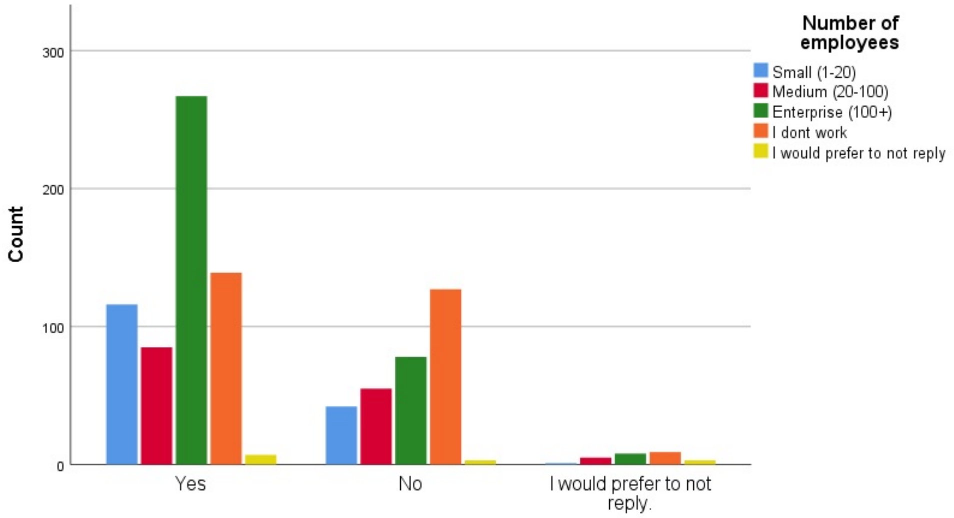


Figure 22: If the users have knowledge about cyber security regulations by the number of employees.

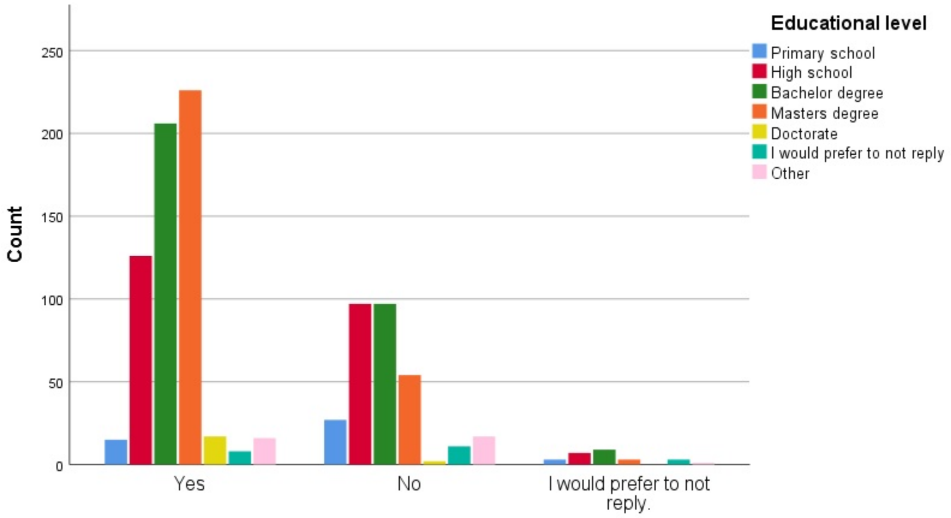


Figure 23: If the users have knowledge about cyber security regulations by educational level

Figure 23 shows that there is a clear difference between the educational groups. The higher education, the higher knowledge about security regulations. Compared to the other results, this question was independent of the area of living, but it had a clear connection to educational level. We saw from the demographic statistics that the area of living and educational level were closely connected, but here these two attributes are differentiated. That means that even if people in rural area er less educated, they do not have a lower level of knowledge than the other groups. Zooming in on the results, by selecting only the people in the rural areas, we found that there is a difference with the group of people living in the rural areas (Figure: 24).

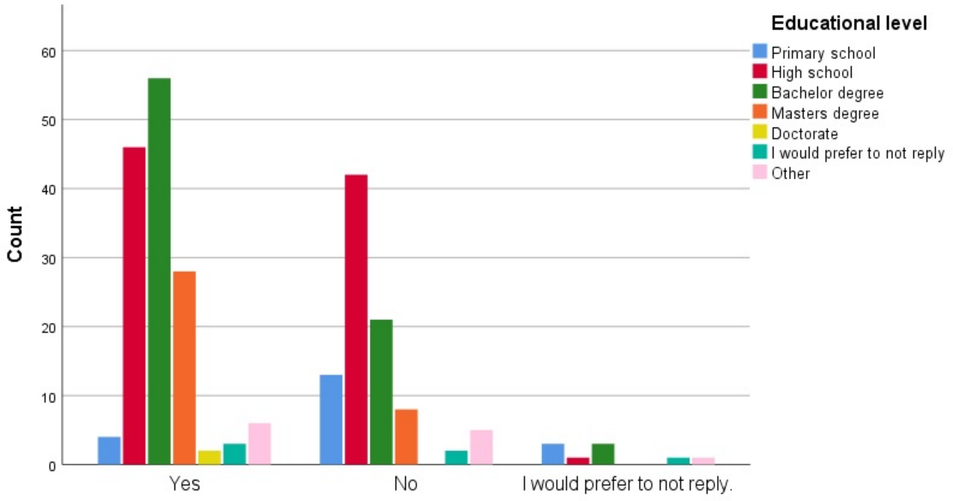


Figure 24: If the users have knowledge about cyber security regulations by educational level, for the rural areas only.

Figure 24 shows that the only group that correlates with the overall result for the rural areas are the users with an educational level less than a bachelor degree, that knows less than average. The users with a bachelor degree or more, that live in the rural areas, they compensate for the very low level of knowledge among the others who live in the rural areas. Hence, we assume that the educated people in the rural areas must know more than their corresponding group in other living areas.

6.3.5 Summary of knowledge

When evaluating the general level of knowledge for the subscription owners of Eidsiva bredbånd, we noticed that there is a difference among the users in the self-evaluated level of knowledge. Men have a perception of a higher knowledge level than women, that our results can confirm. Also, the level of knowledge is different between the groups, such as the working environment, that highly influences the general level of knowledge. However, even if users in the rural areas score themselves lower in self-evaluating their knowledge, we found no evidence for them having a lower level of security knowledge. In fact, people with higher education living in rural areas, scored themselves better in the level of knowledge than their educational group in other living areas.

It is difficult to measure the level of knowledge when we do not know how relative the scale is and what to compare the results with. Self-evaluation through questions are therefore a relative scale that both we and other such as NorSiS have used. What we did find, is that self-evaluation of knowledge is highly subjective and that it is a questionable parameter to use when measuring knowledge. The NorSIS report states the level of knowledge about cyber security in Norway is good, but that it has not changed during the last years. A question such as "Do you know what cyber security is?", is a good baseline, but is highly subjective. That about 90% of the users claim to be aware of online threats, while 77,8% claims to know what cyber security is, and 65% if the users were aware of any regulations, indicate that most users have a feeling of what cyber security is, but that their actual skills are highly subjective and also may not be as good as they think. The subscription owners of Eidsiva rates themselves to be highly knowledgeable. If the true level of knowledge is, in fact, higher for subscription owner of Eidsiva, it is important to identify the reason behind that. Especially because we see that the subscription owners had a lower interest towards ICT and that they were more positive towards cyber security than the rest of the population. The next sections measure how the level of knowledge correlates with trust and risk-evaluations.

6.4 Cyber security risk evaluation

In the previous section, we mentioned an analogy, where we compared the knowledge of cyber security to the knowledge of cars. We also know that men consider themselves to be better drivers, but in fact they are more involved in accidents than women. We question if this also is transferable to cyber security. Security awareness is closely connected to the perception of risk and trust. Studies have shown that our willingness to take risks is closely connected to the level knowledge [18]. The more we know, the more risk we are willing to take. This is due to our ability to overestimate our skills. When the government and security workers aim to let the population gain more knowledge about security, it is a paradox if more knowledge leads to more cyber security incidents. However, we also know that we learn from the mistakes we make and from the incidents we are involved in [13]. Hence, knowledge about risks influences security awareness. Therefore we measured the perception of risk by asking about; perception of threats, how worried people are about using online services, how they associate risk with online services, how secure they feel themselves and if security incidents have made them more cautious and aware.

6.4.1 Self-evaluation of risk when assessing online services

This perception of being aware, the level of knowledge and the perception of taking risk are measured in our next question of whether "The users feel themselves capable of assessing what is safe and not safe". We scaled the replies in 5 levels of agreement from fully disagree to fully agree. The replies are based on a self-evaluation and therefore the results are also here highly subjective. However, it gives a good baseline of measuring the different perceptions of taking risks between the groups, when comparing how worried they are to how much risk they are willing to take.

72,1% replied that they fully agreed or partly agreed to be capable of assessing what is safe and not safe. As a face-value, this is a significantly different result than the NorSIS report, where only 57% answered "Yes" to the same question. However, NorSIS gave the users only "Yes", "No" and "Don't know" options, while we gave the users 6 options. We are assuming that our scale options made more users capable of answering more precise and therefore, fewer users replied "Don't know" and placed themselves in the middle of the scale. NorSIS had 18% "Don't know" and we had 2,9% "Don't know" replies. We see in Figure 25 that men, in general, feel more capable than women in assessing what is safe and not safe.

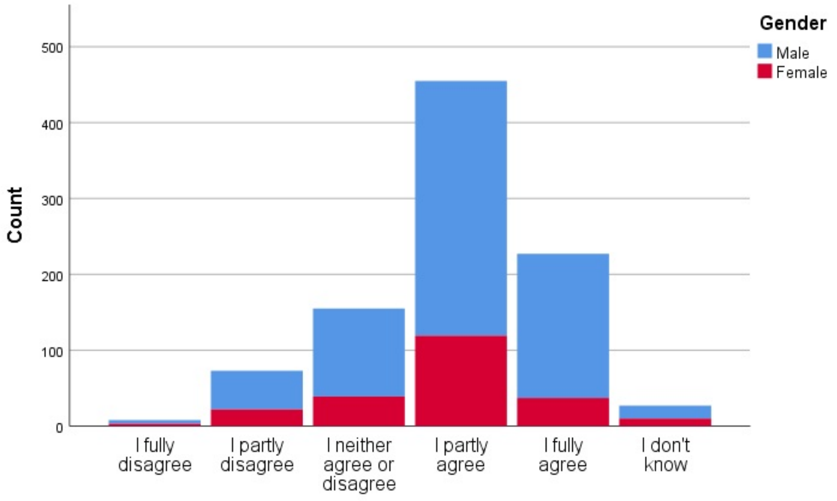


Figure 25: How much the users agreed in being capable to assess what is safe or unsafe to do online, in relation to gender

The ANOVA test shows a variance where 73,6% of the men and 67,8% of the women partly agreed or agreed to be able to assess their safety. However, our sample contains a much higher rate of elderly people that affect our results.

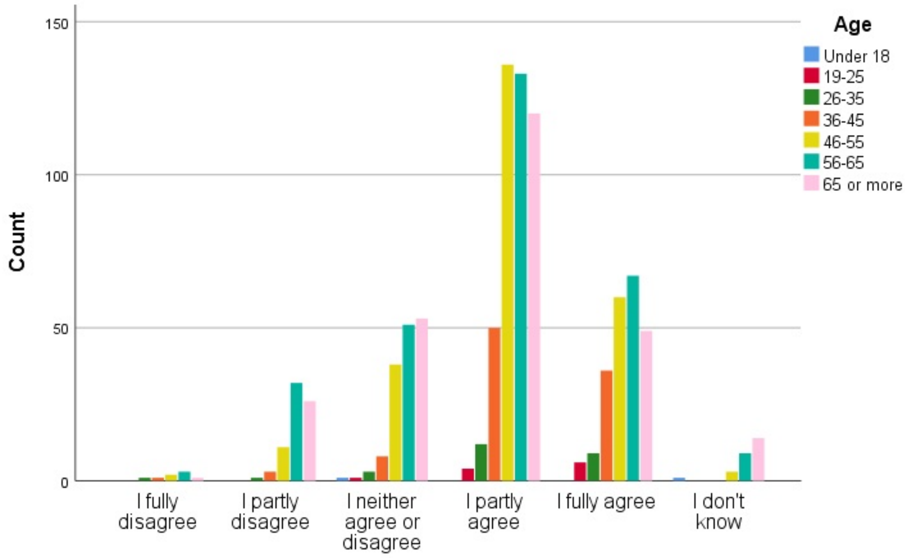


Figure 26: How much the users agreed in being capable to assess what is safe and not safe, in relation to age.

We see a similar pattern as we need when measuring knowledge regarding age (Figure: 26). 71% of the users below 34 years and 66% of the users above 55 years answered that they to partly or fully agreed in their capability of assessing what is safe and not safe. Comparing this result to the NoRSIS report, their results were that 67% of the users below 34 years and 44% of the users over 55 years felt capable of assessing what is safe not.

Here, it is considered that our sample is over-represented by elderly men and that we know that men and younger people consider themselves to be more capable of assessing what is safe and not safe. When taking that fact into account, our results seem to correlate with other surveys such as the NorSIS report [13].

An interesting fact is that we did not find any deviation from the normalization graph by looking into the variations within the groups of the area of living, educational level and working environment, as we did when measuring knowledge.

6.4.2 Measuring the level of concern about cyber security

The level of concern is connected to many elements such as knowledge, trust and fear. Given the fact that the users consider their the level of knowledge relatively high, then it is reasonable to believe that their fear is not connected with not knowing. NorSIS states in their report that the level of fear is increasing and that it is reasonable to be concerned about a decreasing level of trust [13]. When we ask Eidsiva's subscription owners about how worried they were about being exposed for cyber security incidents, we assumed that we measured the level of fear and therefore we also assumed that we measured trust. On the other hand, not being worried can also indicate that people do know the risk. However, maybe they do not care about or fear the consequences, but still lacks or have trust in the services. These questions about concern are therefore setting a subjective baseline of fear. We chose to focus on typically security incidents similar to the NorSIS survey, in order to compare the results with the subscription owners of Eidsiva and to our demographic attributes. We scaled how worried they were in 5 levels from 1 - not being worried at all to 5 - being significantly worried.

We asked the users about how worried they were about 1 - Getting their credit card stolen, 2 - Having their identity stolen, 3 - To have personal files lost and 4 - Being manipulated online. The overall result shows that all question had a similar result of how the internet subscription users perceived the risk. In average, the users were over average concerned. Figure 27 shows the distribution of the responses where the normalization graph is slightly skewed towards being worried.

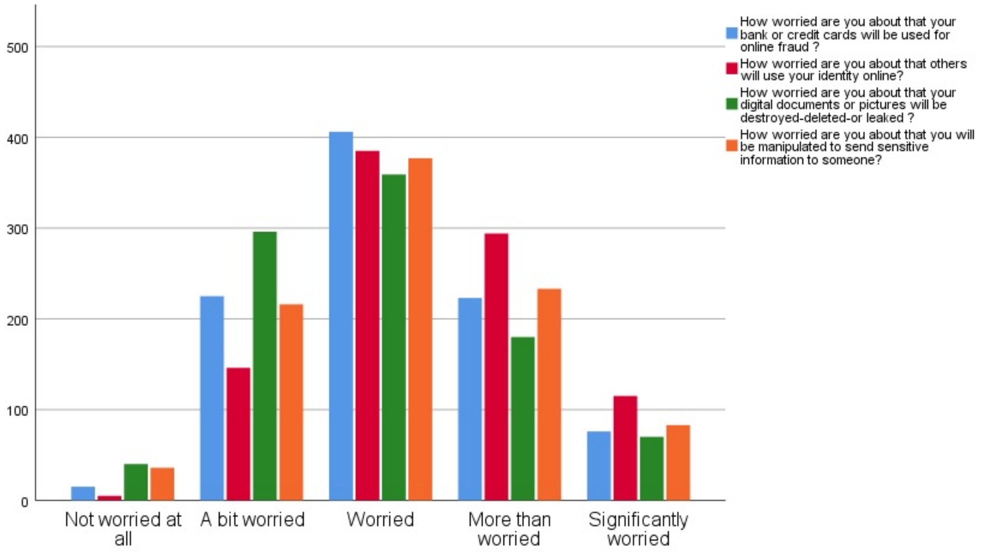


Figure 27: 4 questions to measure their concern about threats

In respect with relations to the demographic attributes, the correlations tests showed very little variation between the groups. However, women tend to be more worried than men for having there credit cards stolen or having their files lost. Concerning the question of having their credit cards stolen, 31,6% that replied to be over average worried or significantly worried, where divided by gender there were 39,5% women and 29,1% men (Figure: 28). A similar distribution also applied to the fear of having their files, such as digital documents or pictures lost (Figure: 29). In total 26,4% were over average or significantly worries that their files could get lost, where divided by gender there were 34,3% women and 23,9% men. This significant variation in the distribution was not found for the users' concern about identity theft or manipulation.

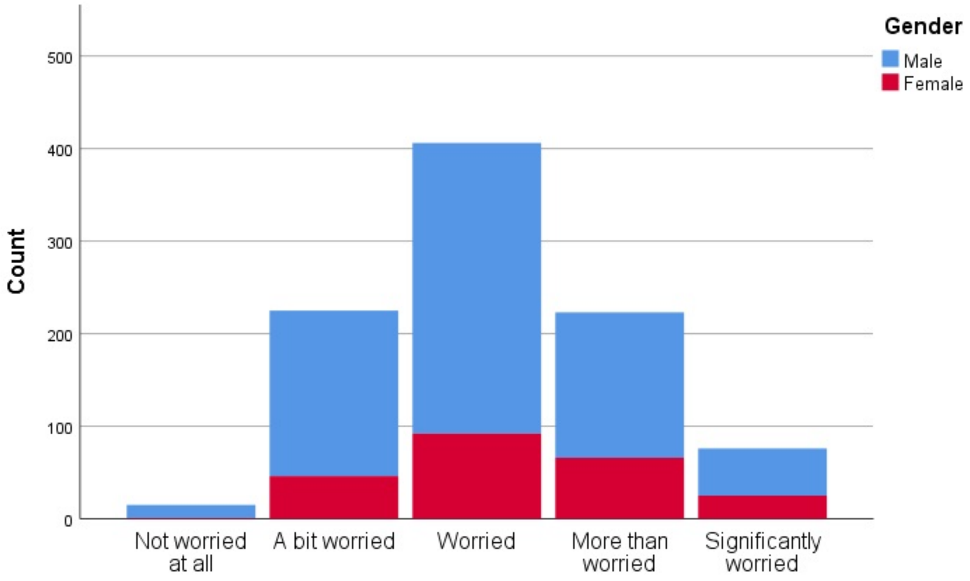


Figure 28: How worried the users are about their bank or credit cards will be used for online fraud

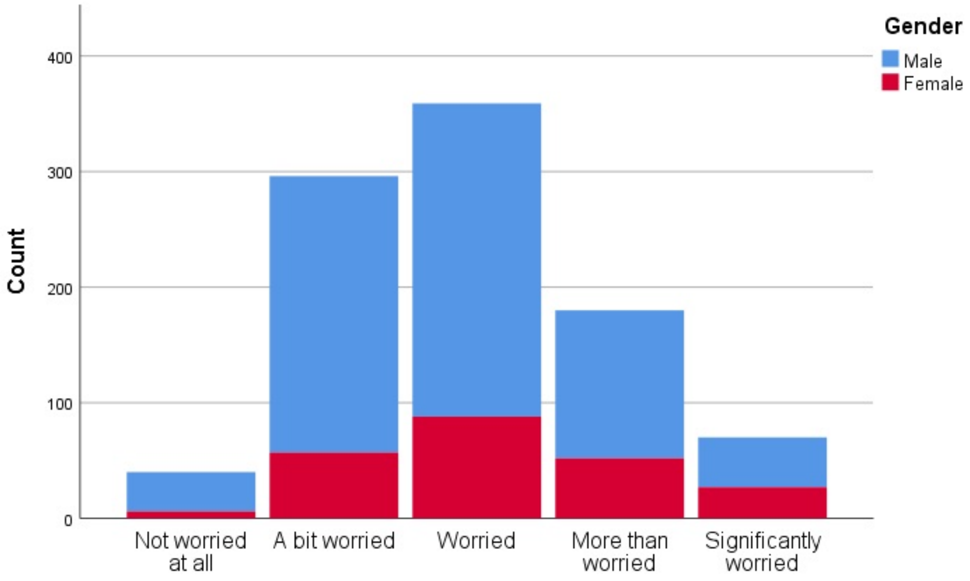


Figure 29: How worried the users are about their digital documents or pictures will be destroyed-deleted-or leaked

We also asked the users how concerned they were about identity theft, where 43,3% responded that they were over average or significantly worried. However, this question showed no significant variance within the demographic attributes (Figure: 30).

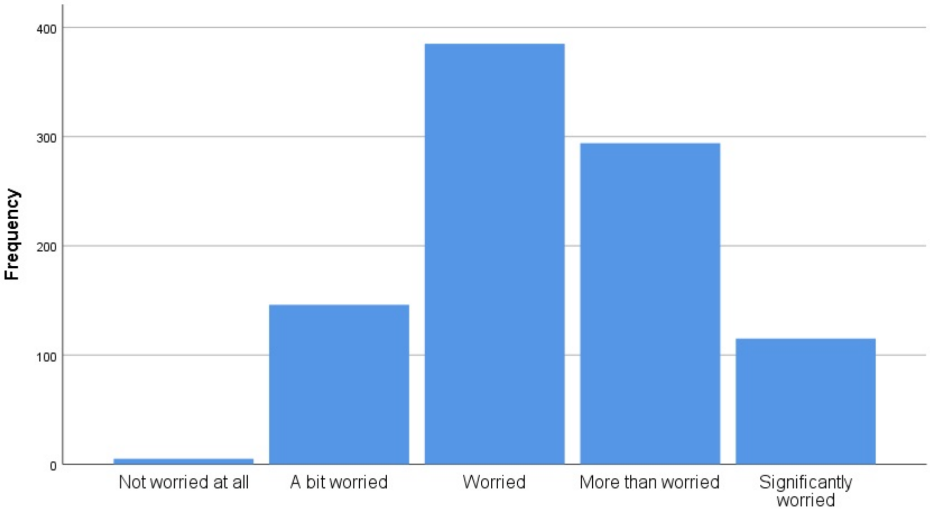


Figure 30: How worried are you about others will use their identity online

The last question we asked about how concern was; "How worried are you about that you will be manipulated to send sensitive information to someone?" 33,5% replied to be over average or significantly concerned. With respect to our demographic groups, there was in this case, no variation between genders. Contrary, there is a significant variance in age and employment sector. Filtering out the employment sector "retired", resulted in a correlation variance to age only.

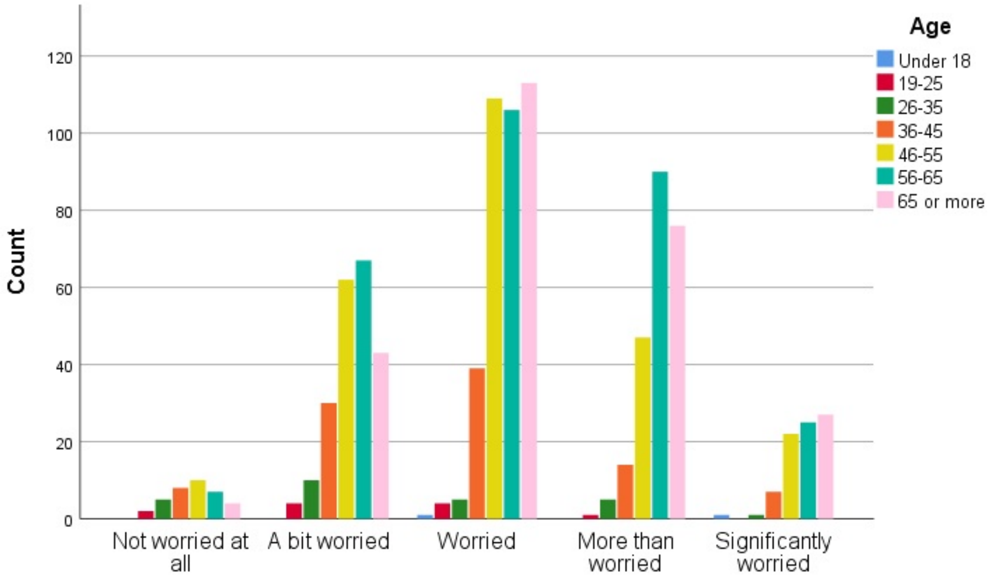


Figure 31: How worried the users are about that they will be manipulated to send sensitive information to someone

33,5% of the total group claimed to be over average or significantly worried about online manipulation. Figure 31 shows that it is not a significant variance for retired users only, but the result shows that the level of how worried users are about this, are very different for all age groups. It is neither a consistent tendency that increasing age results in an increasing level of concern. Young users below the age of 25 years seem to have very little concerns, while the group with the age of 26-55 is in average less than average worried. However, the people from 56 and older, seem to be more worried than the other groups.

The reason for the variation in the replies for the last question, in particular, is not known based. However, we see that these age groups are correlating with the age of the digital natives (20-) and the users that have been involved in the digital age from an early age (20-40). Why, in particular, online manipulation is a greater concern than identity theft and online fraud, is assumed to be connected with life experience and social factors.

6.4.3 Perceptions of risks

It is natural to believe that most people answer similar to questions about risk evaluation as to their concern about cyber security assessments. However, as previously mentioned, it is known that putting ourselves into risk, is necessarily not the same as being worried about it. One of the main objectives of the survey was to discover if there were any differences in the perception of risk among the different groups of people. Hence, we asked them about how much risk they associated with different activities. We asked them to rate the risk from 1 to 5, where 1 is a very low risk and 5 is a very high risk.

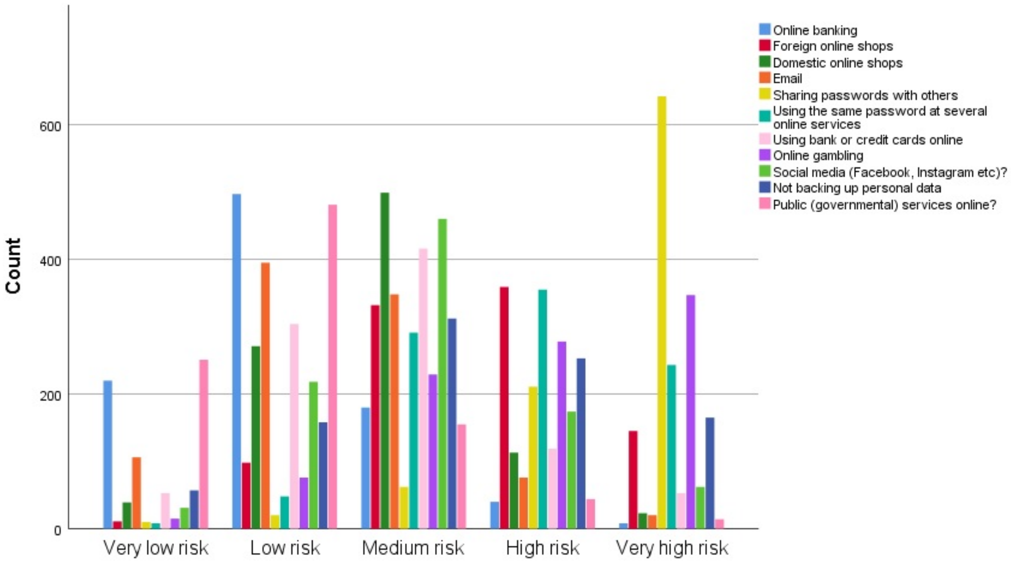
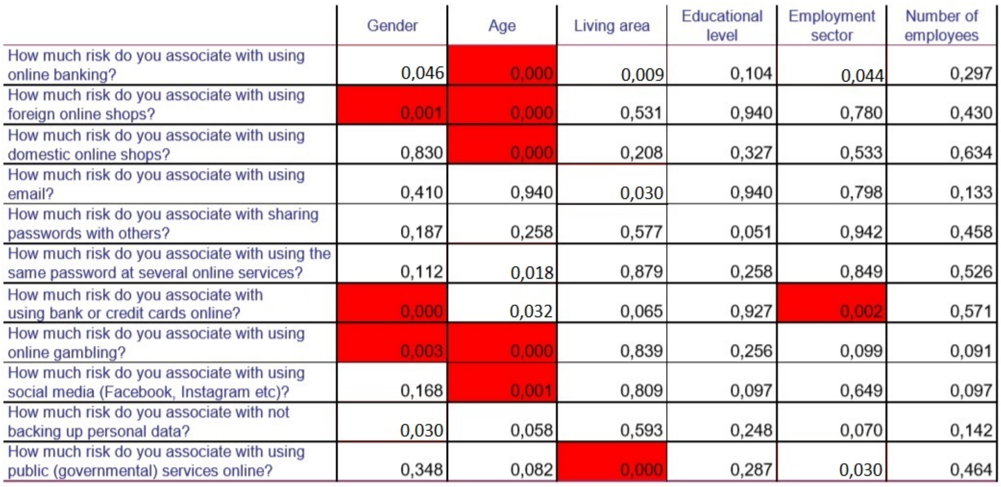


Figure 32: Association of risk

Figure 32 shows that there is a significant difference in how the users perceive risk. As a general fact, this difference indicates that the users are highly aware that there are different levels of risk associated with different activities. For example, sharing your password with someone you trust is considered a very high risk, while using online banking services is on the other hand not considered to have a high risk.

Figure 33 shows the questions we asked in our survey and how much variance there were within our demographic groups. We see that age, in particular, is a significant differentiating factor in how the level of risk is perceived among the demographic groups (marked red).



	Gender	Age	Living area	Educational level	Employment sector	Number of employees
How much risk do you associate with using online banking?	0,046	0,000	0,009	0,104	0,044	0,297
How much risk do you associate with using foreign online shops?	0,001	0,000	0,531	0,940	0,780	0,430
How much risk do you associate with using domestic online shops?	0,830	0,000	0,208	0,327	0,533	0,634
How much risk do you associate with using email?	0,410	0,940	0,030	0,940	0,798	0,133
How much risk do you associate with sharing passwords with others?	0,187	0,258	0,577	0,051	0,942	0,458
How much risk do you associate with using the same password at several online services?	0,112	0,018	0,879	0,258	0,849	0,526
How much risk do you associate with using bank or credit cards online?	0,000	0,032	0,065	0,927	0,002	0,571
How much risk do you associate with using online gambling?	0,003	0,000	0,839	0,256	0,099	0,091
How much risk do you associate with using social media (Facebook, Instagram etc)?	0,168	0,001	0,809	0,097	0,649	0,097
How much risk do you associate with not backing up personal data?	0,030	0,058	0,593	0,248	0,070	0,142
How much risk do you associate with using public (governmental) services online?	0,348	0,082	0,000	0,287	0,030	0,464

Figure 33: P-value correlation score of risk association questions

For online banking, we see that 75,9% of all users considered these services to have low or very low risk in using. Figure 34 shows that there is a general negative skewness to the question for all age groups, but the ANOVA tests showed a significant difference among the elder people. They consider it a higher risk of using online banking than younger people. In comparison the NorSIS survey, 52% of the national population associated low or very low risk with online banking. Therefore, our results are probably affected by the high average age in our sample.

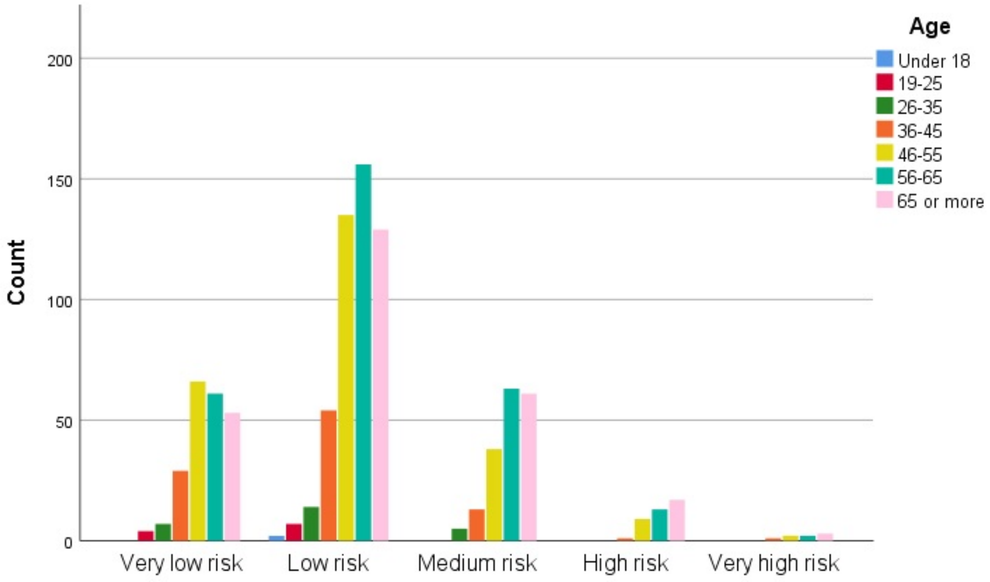


Figure 34: How much risk it is associated with online banking, distributed by age

We see a similar demographic pattern for the users when they did a risk evaluation of online shopping on foreign websites. 53,3% of them considered it to be a high or very high risk to shop on foreign websites. Here, the elderly people considered it to be more risk associated with it, as 57,3% of the people above 56 years considered it a high or very high risk (Figure 35).

An even more significant variance, is that 51,0% of the males and 60,0% of females, had a high or very high risk associated with foreign online shopping.

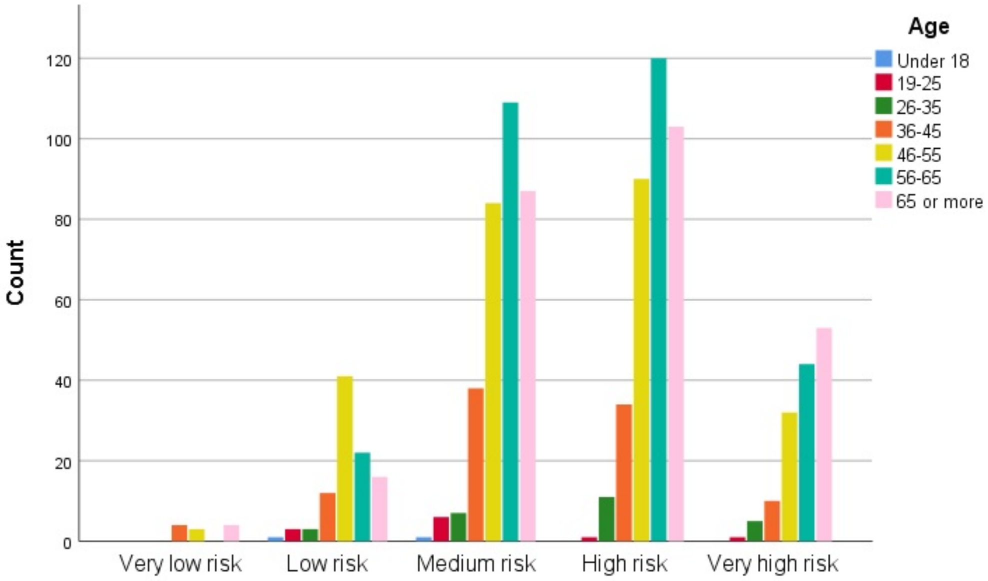


Figure 35: How much risk it is associated with foreign online shopping, distributed by age

In comparison, domestic online shopping is considered much safer, where only 14,4% of the people above 56 years considered it to a high or very high risk, and 10,8% of the people below 56 years had a similar risk perception of domestic online shopping (Figure: 36).

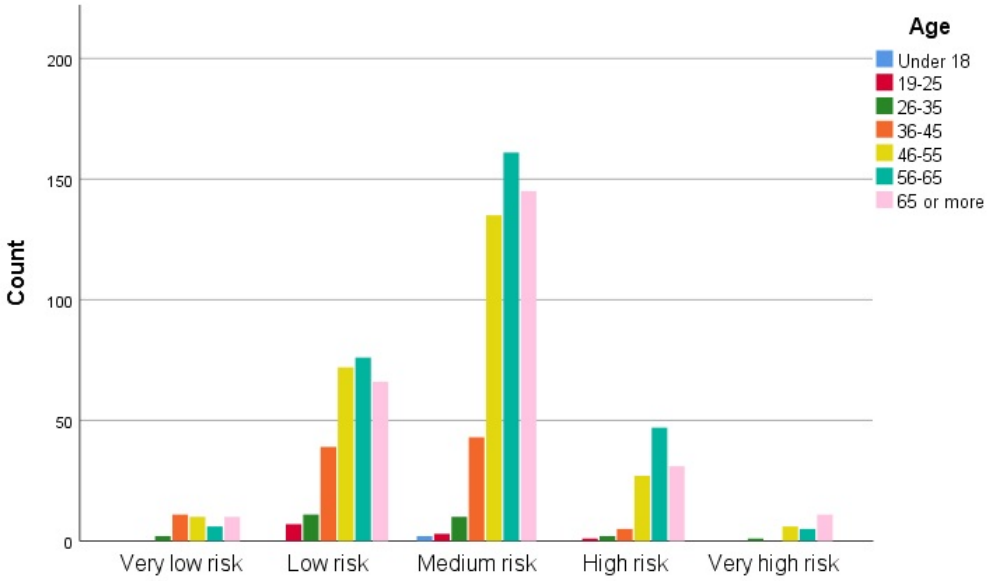


Figure 36: How much risk it is associated with domestic online shopping, distributed by age

Another risk perception question we asked the users about, was how much risk they associated with online gambling. In general, 66,1% of the users considered it a high or very high risk to do online gambling. In these high-risk groups, the age distribution consisted of 71,5% of users above the age of 56 and 58,3% of users below the age of 56 years (Figure: 42). Out of these, there were also 64,9% men and 70,0% women. Once again, age and gender variances indicate that the overall result is affected by our sample. This is also confirmed by comparing it to the NorSIS survey. Here, 43% considered online gambling with high or very high risk.

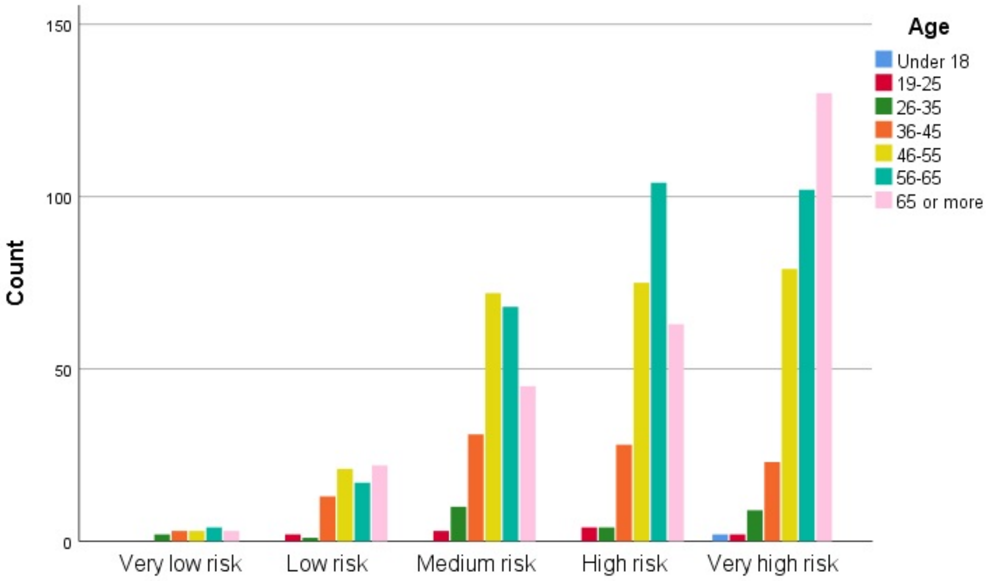


Figure 37: How much risk it is associated with online gambling, distributed by age

For the questions concerning online banking, online shopping and online gambling questions, we identified a connection to the action of handling money. For these services that include a direct handling of their money, we see a similar variation, where the older generations consider it a greater risk. In particular, elderly women seem to have a greater perception of higher risks than the other groups. This is confirmed when asking about the risk evaluation of using bank or credit cards online (Figure: 38). Here, we can also see a small variation within the age and gender groups. 18,2% evaluated it as a high or very high risk, where within this group there were 16,6% men and 23,0% women. 15,5% of the people below the age of 56 and 19,3% above the age of 56 also considered using bank or credit cards online as a high or very high risk. It is also noticeable that the people working with agriculture had the greatest risk evaluation of using bank or credit cards online (25,0%). This variation existed for the agriculture working sector only, that we did not see in any of the other questions related to risk evaluation. We did not find any explanation for this distribution.

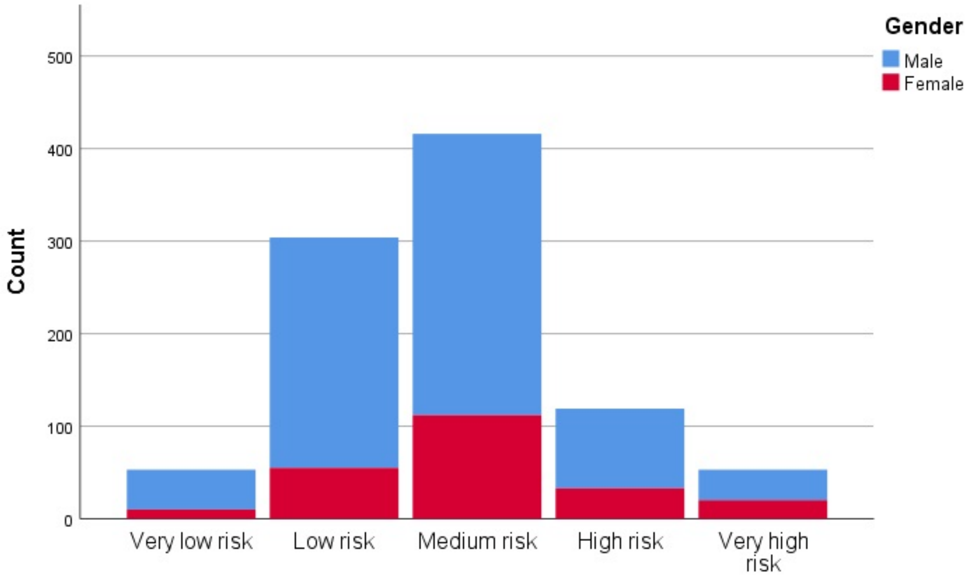


Figure 38: How much risk it is associated with using bank or credit cards online, distributed by gender

For the other questions where we asked about risk evaluations, that did not concern the handling of money, we did not see these deviations in the correlations.

The risk perceptions of using email, sharing passwords and data backups are correlating for all groups. However, most people score these questions a bit differently than we excepted. Using email has historically been one of the most popular channels to spread computer virus and manipulate people. Surprisingly, only 10,1% associate using email as a high or very high cyber security risk, while 53,0% associate it with a very low or low risk (Figure: 39). There were no age or gender variations for this questions, that indicates that the subscription owners of Eidsiva evaluate email as a safer service than the rest of the Norwegian population. NorSIS presents that 21% of the Norwegian population considers it a high or very high risk and 40% as a low or very low risk.

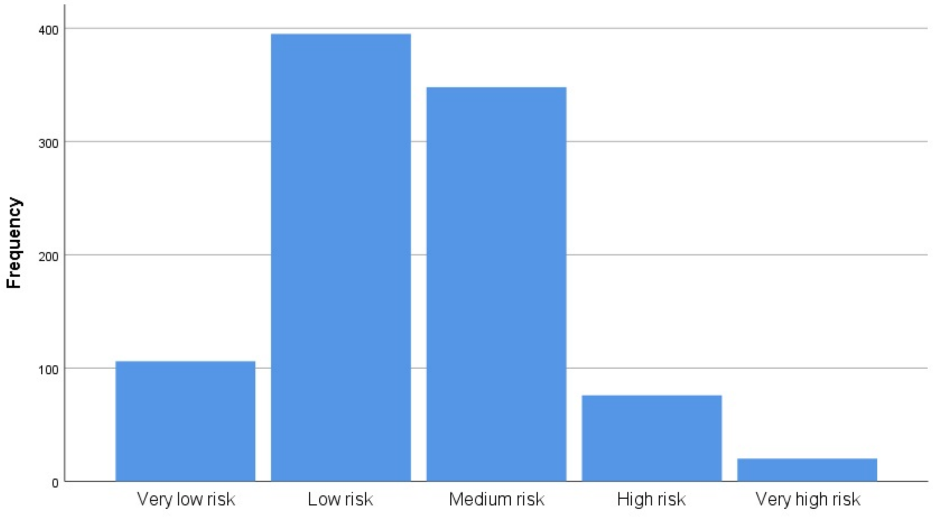


Figure 39: How much risk it is associated with using email

When it comes to passwords, 90,2% claims that is a high or very risk of sharing a password to someone you choose to trust, while only 63,3% claims that is a high or very high risk in not using the same password on different websites (Figure 40).

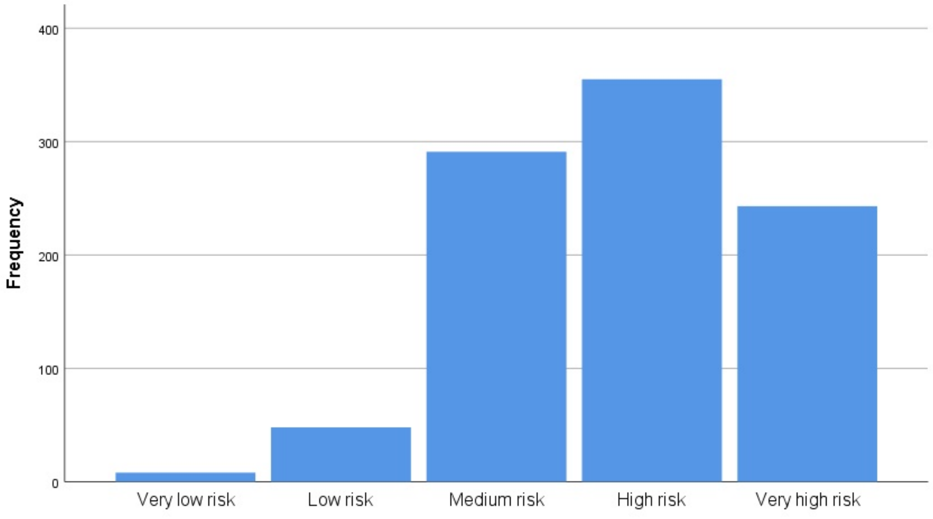


Figure 40: How much risk it is associated with using the same password at several online services

We also compared these results to the NorSIS report. Here, 55% of the users considered not using the same passwords on multiple websites as a high or very high risk. 76% replied that password sharing is a high or very high risk. Since we did not see any correlation to demographic attributes in our data-set, this indicates that the subscription owners of Eidsiva see a greater risk concerning the use of passwords. However, common for both surveys, is that for these two questions, the difference in percentage point between the questions, is about similar. We question how much difference there is in taking risks by sharing a password with someone you trust, or not using separate passwords for different websites. Hence, as a curiosity, we isolated the data to only people with a master degree or a PhD degree that is working in the ICT sector. In that group, 97,7% considered it a high or very high risk to share passwords. Out of this group of 43 people, 72,2% also considered not using separate passwords as a high or very high risk. Therefore, ICT professionals, do also consider password sharing with someone you know as a much greater risk than using the same password on multiple website accounts.

Data backup is a different kind of associated risks than the previous risk evaluation questions. We asked generally how much risk they associated with not having their data backed up. Backup routines have changed for the last decade. Many people now trust their cloud services as their primary file location, with or without an additional personal backup. However, 22,7% answered to have low or very low risk evaluation of not having a data backup. On the other hand, 44,3% replied to have a high or very high risk evaluation of not having data backups (Figure: 41). The normal distribution correlates with the NorSIS results.

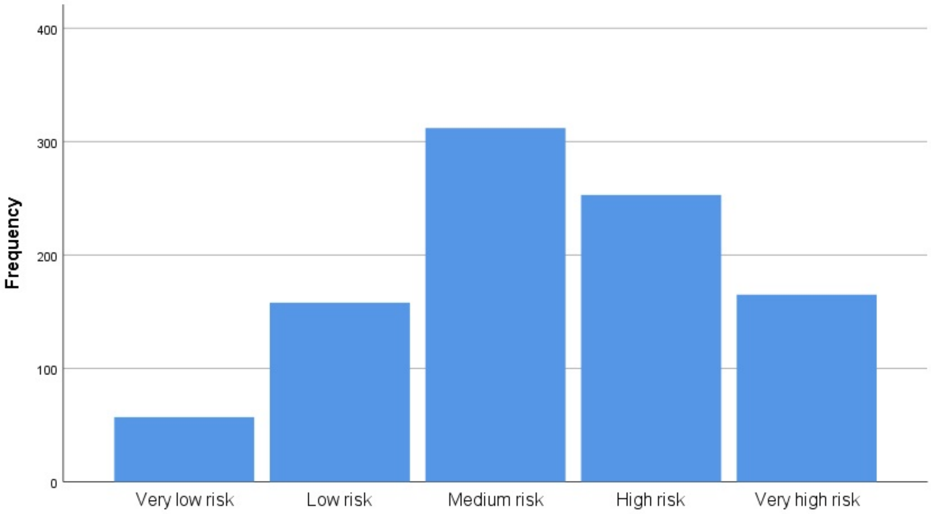


Figure 41: How much risk it is associated with not backing up personal data

The previous questions about risk evaluations measured how the people value their assets. Another aspect of risk evaluation is how they value social relations and trust. Asking the people about how must risk they associate with social media, again opens up for multiple interpretations in risk evaluations. Some of the interpretations are for example privacy risk, harassment risk, the risk of being manipulated or the risk of software exploitation. We assume that most people in our survey associate social media with non-technical risks. One of the reasons for this, is that we see a clear connection to the age groups for this question.

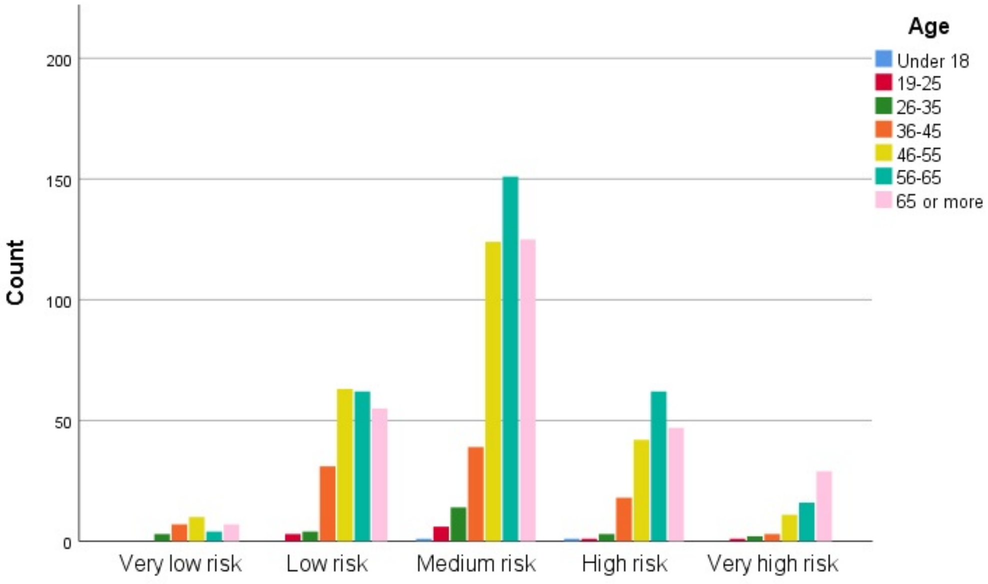


Figure 42: How much risk it is associated with using social media, distributed by age

Figure 42 shows that 25,0% claims to associate social media with high or very high risk, while 26,4% associated with low or very low risk. 22,9% of the people above 56, 29,2% of the people 46-55 and 38,7% of the people from 36 to 45 replied to associate a low or very low risk with this. Hence, there is a tendency that increasing age is increasing by the level risks associated with social media. NorSIS does not present the age distribution in their results, but their national results are different than ours. This leads us to state that the subscription owners of Eidsiva are evaluating the risks to be less than the national population (50% replied high or very high risk). Since the higher age seems to increase the risk evaluation, and the subscription owners of Eidsiva has a high average age, this result of low risks evaluation, shows that the subscription owners of Eidsiva have a different perception of risk than the rest of the population.

Correspondingly, our sample replied similarly to the question of "How much risk do you associate with using public (governmental) services online?" NorSIS presented in their 2018 report that 21% of the population associate a high or very high risk in using public services. In comparison, the users in our sample replied that only 6,2% had a similar risk evaluation. However, NorSIS reported that 44% considered it a high or very risk, while for the users in our sample, 77,5% associated very little risk with that (Figure: 43). Here, our result showed no variation between the groups of age and gender. Hence, this result also indicates that there is a finding in our sample where their general evaluations of risks are low.

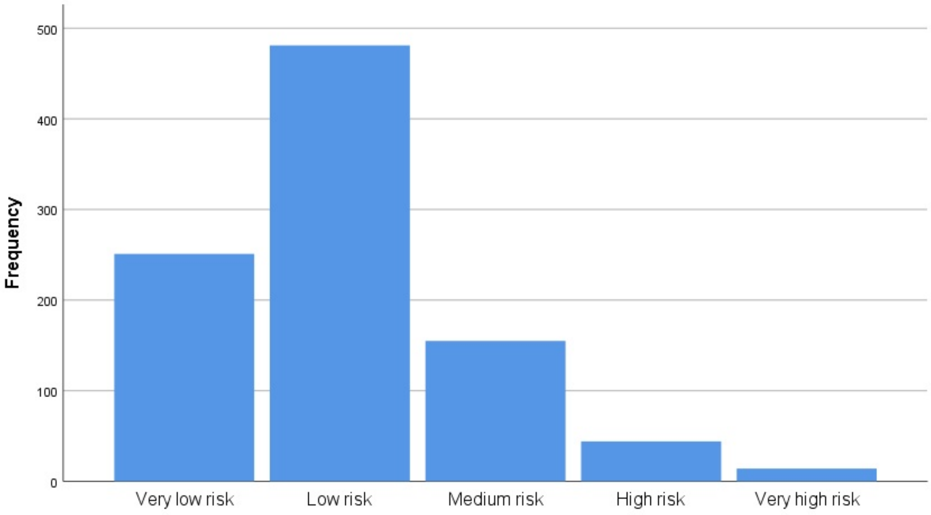


Figure 43: How much risk it is associated with using public (governmental) services online

We did neither find any variations between the demographic groups except for the living area. This fact emphasizes that this question is highly related to the area of living. By all questions related to risk evaluation, this was the only one that had a variance toward living area (Figure: 44).

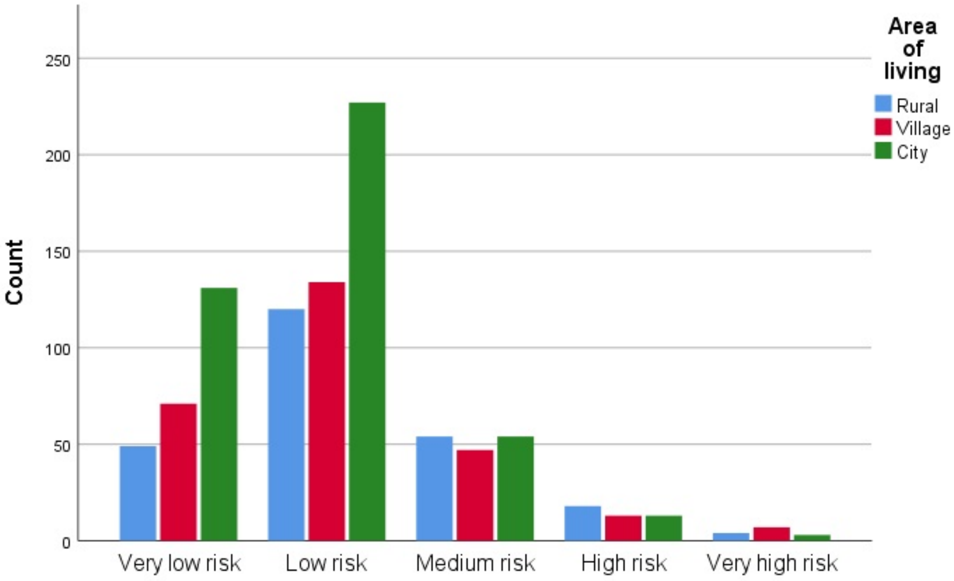


Figure 44: How much risk it is associated with using public services online, distributed by living area

We see that the people in the rural areas think that using public services is a greater risk than people elsewhere. In the rural areas, 69,0% associated low or very low risk with public services, while 83,6% of the people in the city replied similarly.

The region our sample is taken from is less populated than other areas in Norway. While comparing our results to the NorSIS result, it is natural to believe the level of risk evaluation is connected to the density of the population, since our sample has a much higher trust to public services than the rest of Norway. However, within our sample, we see the opposite. The people in the city are less concerned than the people in rural areas.

Since these questions about risk evaluations also are connected with trust, they can also be interpreted as how much the people trust the government, their trust in their service provider or if they have a greater trust/bond in the local community. Hence, we realized that the answers to these questions could also be politically motivated, that also is a possible explanation for the variations.

6.4.4 Changing perceptions of risk evaluations

It is reasonable to believe that security incidents make us re-evaluate the risk of using services. A security incident can make us gain more knowledge and therefore also be more aware or raising the level of concern when using a service. If a global massive attack happened, it is likely to believe that it would raise the security awareness of the general public, but it would probably also make us lose our trust in the service. Hence, it is not preferable to become a victim of a crime or any other violations in order to gain more security awareness. However, we claim that learning by experience contributes to a higher security awareness. For that reason, we made a general question about this and asked: "Has information concerning threats or hacking in the past made you stop using an online service?"

69,9% answered that they changed their usage pattern or stopped using a service due to a security incident. These reply options in this question are a bit more nuanced than in the NorSIS survey, where the users were not given the option of whether they changed their patterns. Therefore, we also see that the numbers are very different (29% answered "Yes"). In respect of correlations, we see a variance for age, employment sector and the number of employees.

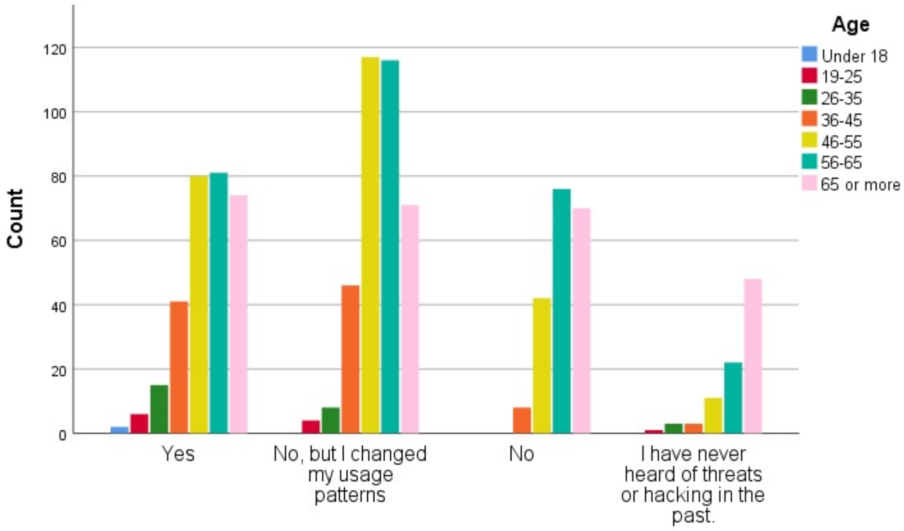


Figure 45: If information concerning threats or hacking in the past made you stop using an online service, distributed by age

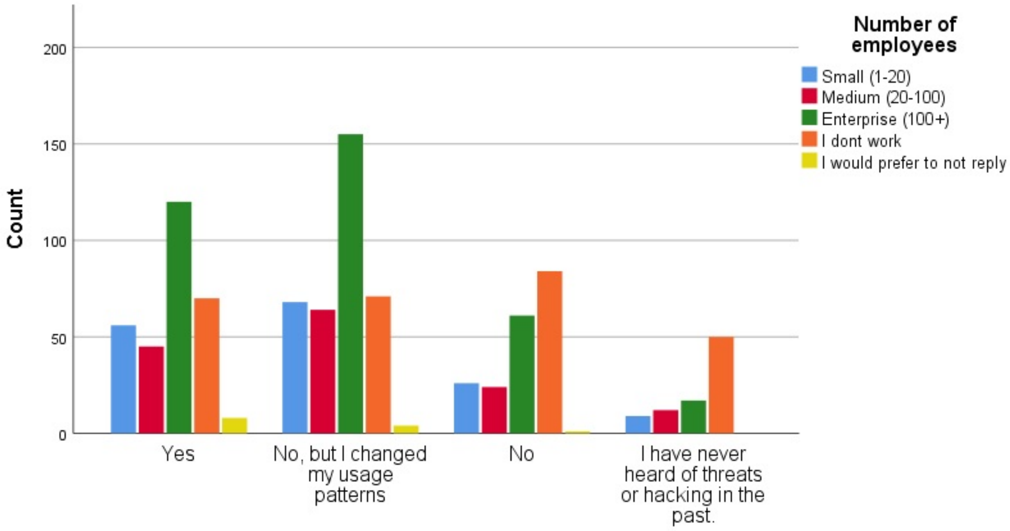


Figure 46: If information concerning threats or hacking in the past made you stop using an online service, distributed by the number of employees

Figure 45 and 46 shows that the variance is due to the age. There is a significant correlation to the age groups of 46 years and above, that indicates that younger people have experienced more security incidents than the older generation. In respect of employment sector and the number of employees, all groups correlate except for the group of retired people. We consider this also an age indicator.

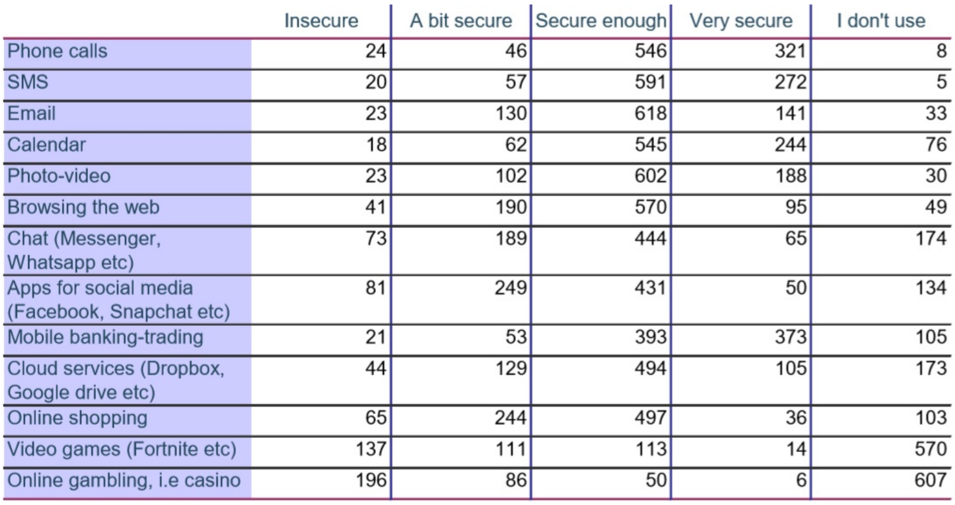
It is a challenge that 33,3% of the population above the age of 45 have never experienced a security incident that changed their behaviour or made them stop using the service. Among the people below 45 years, only 10,9% claimed to have a similar experience.

This indicates that it is more difficult to raise the general level of security awareness for older people than younger people. However, the number of security incidents is obviously also connected with how much they use online services. Therefore, we suspect the usage pattern to be different for the older generation than for younger people. We state that this is because the older users use fewer services than the younger users. This statement we cover in the next section (Section: 6.4.5).

6.4.5 The level of feeling safe

We asked the users how safe they felt when using a number of applications on their mobile phone. This is an additional indication of their risks evaluations, but it also discovers their usage pattern. As we have seen from the previous question, it is likely to believe that usage is affecting the number of security incidents and their security awareness. We chose to focus the usage pattern on mobile devices. It possible that the level of safety is different between computers and mobile phones, that is also seen from other surveys [9]. However, we know from these studies that this question both options cover their usage pattern and their evaluations of risks similarly.

For this question, we gave the users the options of scaling their level safety from insecure to very secure in 4 levels. There were also given an option of not using the service. Figure 47 shows the different services we measured and the frequency table of the replies.



	Insecure	A bit secure	Secure enough	Very secure	I don't use
Phone calls	24	46	546	321	8
SMS	20	57	591	272	5
Email	23	130	618	141	33
Calendar	18	62	545	244	76
Photo-video	23	102	602	188	30
Browsing the web	41	190	570	95	49
Chat (Messenger, Whatsapp etc)	73	189	444	65	174
Apps for social media (Facebook, Snapchat etc)	81	249	431	50	134
Mobile banking-trading	21	53	393	373	105
Cloud services (Dropbox, Google drive etc)	44	129	494	105	173
Online shopping	65	244	497	36	103
Video games (Fortnite etc)	137	111	113	14	570
Online gambling, i.e casino	196	86	50	6	607

Figure 47: Frequency table of the level of safety for different applications

Figure 48 shows a graphical representation of all services, where we see that most applications are considered to be over average secure for the users. Apart from online gambling and online gaming, most people use most services. However, we see two other services with significant differences in usage, that is chat and cloud services.

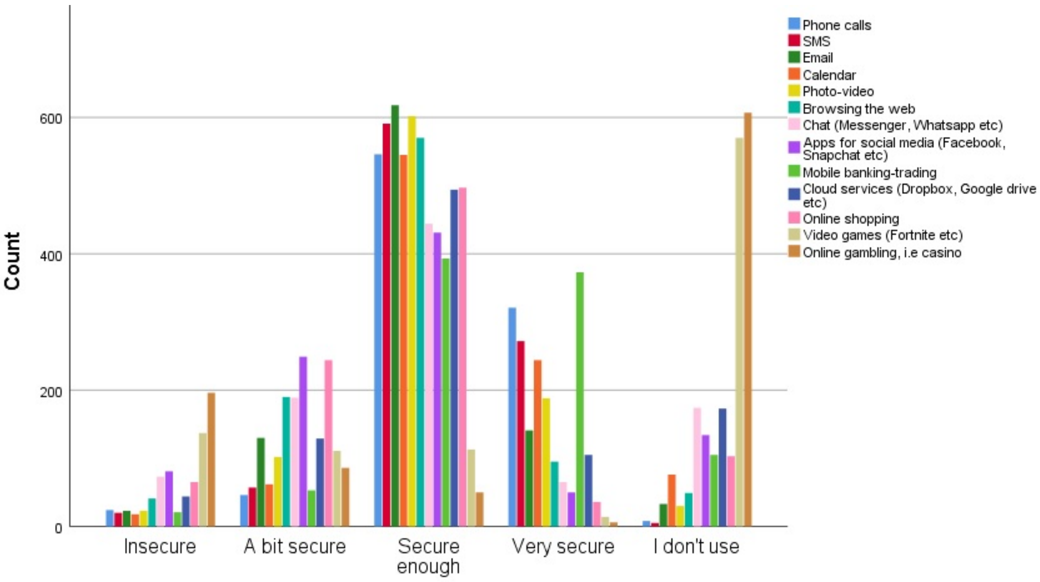


Figure 48: Graphical representation of the level of safety for different services

As we have seen from the previous questions about risk evaluation, there is a strong variation in the results when comparing them with age distributions. However, we see that for the traditional mobile phone applications, such as Phone, SMS, calendar, Photo and online banking, there is no difference in how the different groups perceive their safety and the usage pattern is similar for all age generations. All these applications are commonly used among all groups. Also, in average, around 8% of the users consider all these applications a bit or very insecure. On the other hand, these applications are also standing out as the applications that are considered the most secure (Figure: 48).

For the other groups, there is a significant group of people that do not use these services. Hence, we removed that group when measuring how secure the service is perceived and we grouped the replies into two groups of feeling safe (secure enough, very secure) and not feeling safe (insecure, a bit secure). As a result of that, none of these questions showed any significant difference between the demographic groups.

Using email and browsing the web are also two services that are commonly used, where only 3,5% don't use email and 5,2% don't browse the web. The people that don't use the web on their mobile phones are primarily above the age of 46. However, 99,7% of the users say that they do use their mobile phone for web services such as social media, shopping and banking. We assume they use a separate application than the web browser for that. The level of feeling safe when using these services is high, while 16,8% of the users that are using email and 25,8% of the users that are using browsing feel themselves relatively unsafe. There is a small variance within the age groups, that indicates that the elderly (65+) feel less safe than younger when using email (Figure: 49).

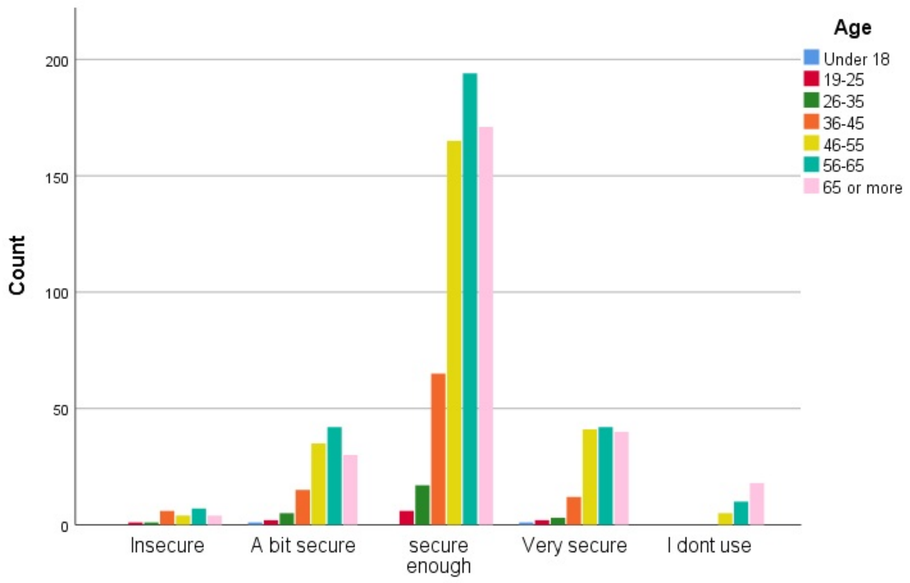


Figure 49: How safe do you feel when using email, distributed by age

However, when it comes to online shopping, 36,7% of the users that used online shopping, do not feel safe (Figure: 50). This applies to all age groups, but there are more elderly people that don't use online shopping. We assume that not feeling safe in this context, is a relative conception according the scale they are presented.

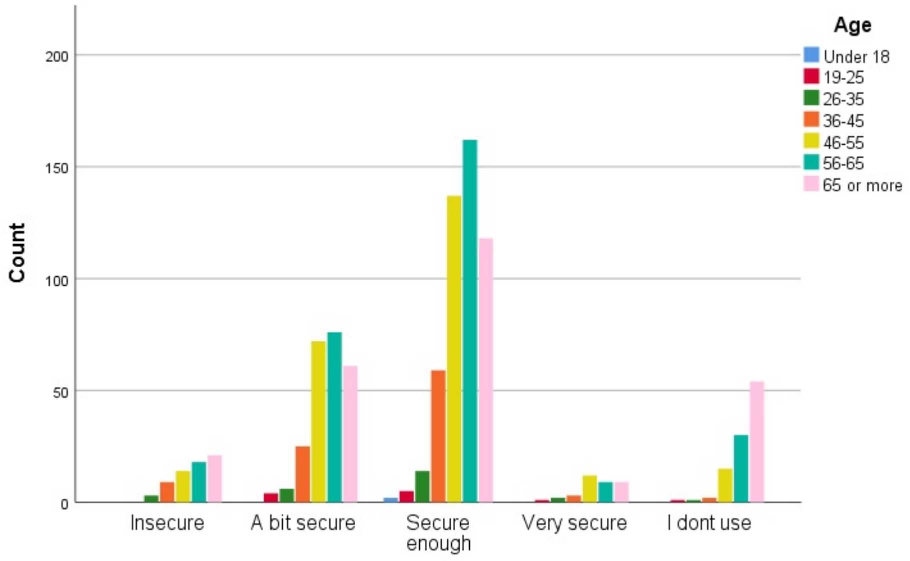


Figure 50: How safe do you feel when doing online shopping, distributed by age

For using cloud services, 18,3% replied that they don't use such services. Also, 22,4% replied that they don't feel safe when using them.

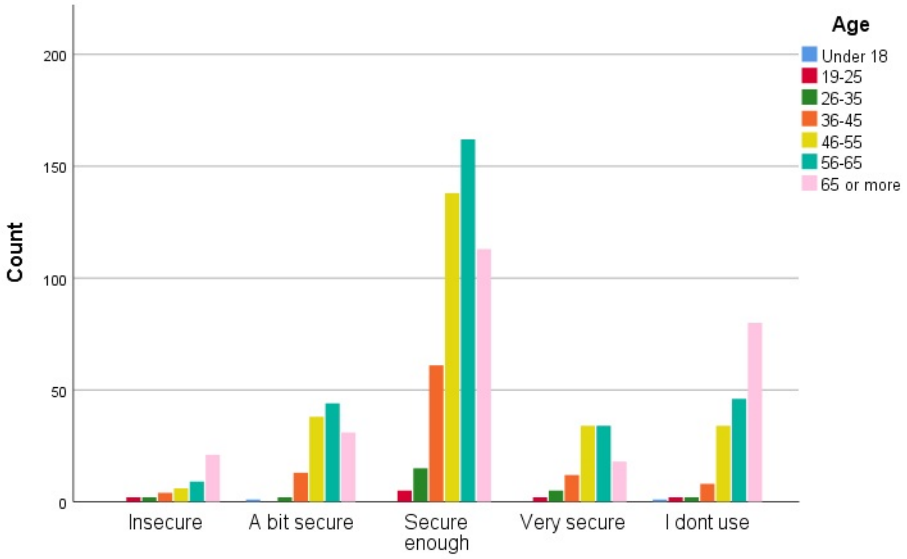


Figure 51: How safe do you feel when using cloud services, distributed by age

Figure 51 shows that we found a variation in the distribution of elderly people and that they are generally not using these cloud services.

Online gambling and online gaming are by far considered as services that are not safe to use. 64,2% don't use online gambling services and 87,7% of people these are above the age of 46. 83,4% of the users that use online gambling doesn't feel safe when using the service.

It is questionable if online gambling sites, in fact, are technically insecure. Hence, we suspect that our users don't associate cyber security technology with the question. Instead, it is possible that they associate the risk of losing money by playing with the insecurity. We do not know if these sites in fact are insecure, if the question was not formulated precisely or if this is a general perception with a lack of knowledge of the gambling companies and their security. We did identify that such questions have to be carefully constructed in future surveys in order to avoid such room for interpretations.

We have not identified any connections to demographic attributes when measuring how safe the people feel when using different services, except that the age is influencing if services are being used or not. This we also see when measuring the feeling social media security level (Figure 52).

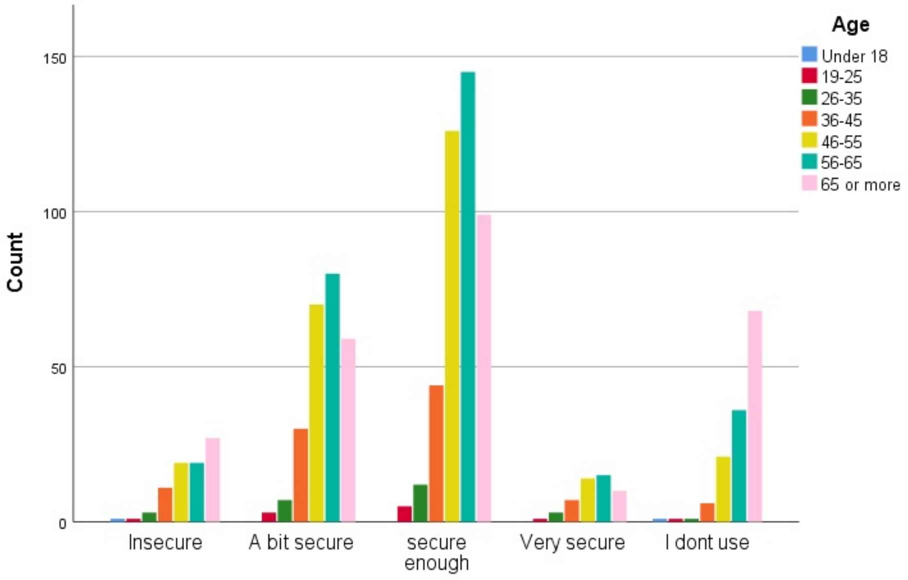


Figure 52: How safe do you feel when using social media, distributed by age

A similar result is also seen when comparing the result to other groups with social media as an example. Figure 53 shows that there is a variance for the people that do not work. This group is over-represented by retired people.

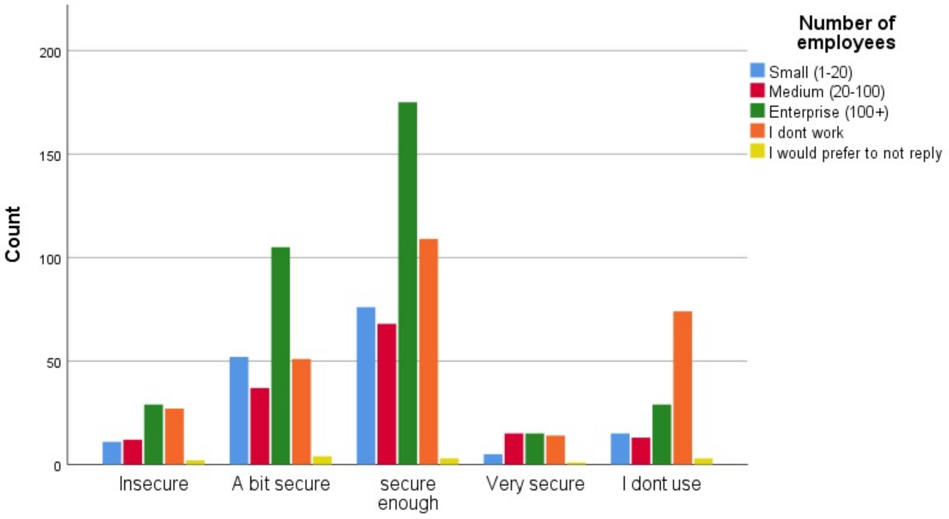


Figure 53: How safe do you feel when using social media, distributed by the number of employees.

Measuring how safe people feel themselves when using online services, did not give any significant indications of variance to demographic groups. However, based on the people that replied that they didn't use the service, this group was correlating with high age. The ANOVA tests also showed a slight correlation between not feeling safe and aged people.

This also indicates that our statement from Section 6.4.4 is correct; That elderly people have reduced usage and they are therefore also less influenced by security incidents.

6.4.6 Security risks in the use of mobile devices

In order to summarize the questions we asked in the previous sections, we asked the users to rate how worried they were about the security on their mobile devices on a scale from 1 to 6, where 1 is not worried and 6 is extremely worried. Figure 54 shows that 57,7% answered to be less than average worried (1,2 or 3).

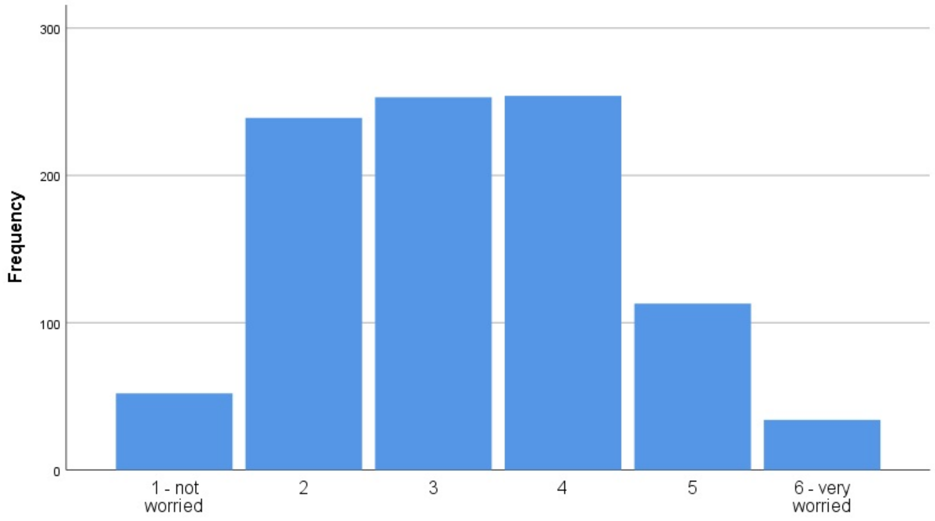


Figure 54: How worried the users are about that their security of on their mobile devices

We saw no variance within the groups of gender, age, living area, education or working environment for this question.

When comparing this result to the questions of how safe the users felt in Section 6.4.5, we see there is a lack of correlation between being generally worried and feeling safe in using specific mobile applications. In general, people felt over average safe in using the specified services, while they feel over average worried about the use of mobile phones in general. These contradicting results indicate that there is something undiscovered within our questions of mobile phone services. One theory is that there are one or more mobile phone services we did not measure. Another theory is that people are worried about the unknown. That means that they don't know what services they are using or they don't have control over the services they are running.

6.4.7 Summary of risk evaluations

In general, the subscription owners of Eidsiva bredbånd are less worried and they are feeling safer than the national population. However, less concern is necessarily not a good thing when it comes to cyber security awareness. Less concern can potentially be caused by high trust levels, low level of knowledge, much experience or a high level of protection knowledge. This is discussed in the next sections of trust in authorities, training and behavioural patterns. On one hand, a lack of concern can be a result of a user experience with little use and a low level of security incidents. The consequence of that would be that the users are unaware and simply living in good faith with no worries. On the other hand, a lack of concern could also indicate a high level of knowledge, high confidence due to training and a generally high level of trust towards service providers, laws and regulations.

6.5 Trust in authorities and user responsibility

This section aims to measure the level of trust the sample of users in Eidsiva have to authorities and what they perceive as their cyber security responsibility. The NorSIS report from 2018 [13] points out the importance of how regulations and authorities are factors in creating trust towards ICT in general. This also includes that the society must accept and understand their responsibilities, their duties and their personal rights under these regulations. We continue this work and further investigates if there are any groups of people that have different perceptions of this. In this section, we measure how much we trust the authorities in being capable of handling incidents, how much of our freedom we are willing to give away in order to feel safe, and the users' general stance towards cyber security responsibilities.

6.5.1 Trust in authorities

We asked the users four simple questions similar to the questions in the NorSIS report, where we aimed to discover the level of trust in authorities. The questions primarily focused on measuring the users' awareness of the responsibility of the police. We asked the following questions:

- What is your most likely course of action if you or a family member are bullied or harassed online?
- What is your most likely course of action if you or a family member are subject to online fraud?
- What is your most likely course of action if your or a family members online identity is stolen?
- What is your most likely course of action if your home computer is infected by a virus?

For each question, we gave the options of: "Do nothing", "Fix it myself", "Ask for help", "Report it to the police" and "I don't know".

The result of the questions deviated from the NorSIS report, but we did not find any variance within any demographic group.

Concerning bullying or harassment, the threshold of reporting an incident to the police is highly individual. However, comparing our result towards the other surveys [13],[9], shows that 53% of the subscription owners would report it to the police, while 29% reported the same in the NorSIS report. A similar difference is seen for online fraud, where 64% of the Norwegian population would report it to the police, while 73% of the users in our survey had a similar opinion. Identity theft is considered to be most frequently reported to the police. 83,8% of the users from Eidsiva bredbånd reported that this is a matter for the police, compared to 72% that said the same among of the national population in the NorSIS report. We also put in a simple awareness question of what the users' actions would be if their computer got infected by a virus. Only 1,3% claimed that this is a matter for the police. Not surprisingly, that indicates that there is a general awareness and understanding among the population that virus infection is not a case for the police.

The subscription owners of Eidsiva bredbånd seem to have more trust in the police. However, it is not known, if a lack of knowledge and a lack of awareness contributes to a higher or lower threshold of reporting incidents to the police. Since the subscription owners of Eidsiva, in general, are more aware of risks and have a higher level of knowledge, we open up for an opportunity that more knowledge, lowers this reporting threshold to the police, based on these results.

6.5.2 Cyber security responsibility

The cyber security awareness is also connected to how much the users feel responsible for their own safety. Some years ago, it was important that users did manual updates and took actions in order to have local backups. In modern society and software, we state that the security routines are more automated than before. Software updates go more automatically, cloud services reduce the need for backups and anti-virus and anti-spam solutions are more or less integrated into many systems, such as the Microsoft Windows operating system. This can cause the users to be less aware of the security solutions that protect them, since it can be perceived as "taken care of" by the service providers. This can also cause the users to put more responsibility on the service providers for protecting them. Also, as a nation, we are protected by the police and the laws, that also can be perceived as an external part that makes sure that we feel safe. This is a trust culture we saw from the previous question (Section: 6.5.1, where noticed that most users trust that the authorities will make us safe without questioning their need for privacy. Hence, we asked the users who they feel is responsible for their security. We gave the users the options of placing the responsibility on: "Themselves", "The service providers", "The authorities/the government" or "Not knowing".

It is a clear opinion that it is a responsibility of the individuals in order to make ourselves safe (75,0%), while 14,3% put the responsibility on the service providers and 4,9% on the government. We did not find any other sources to compare this result with, but we found variations within our demographic groups. Gender, Age and living area seem to have deviations within the distribution of the replies.

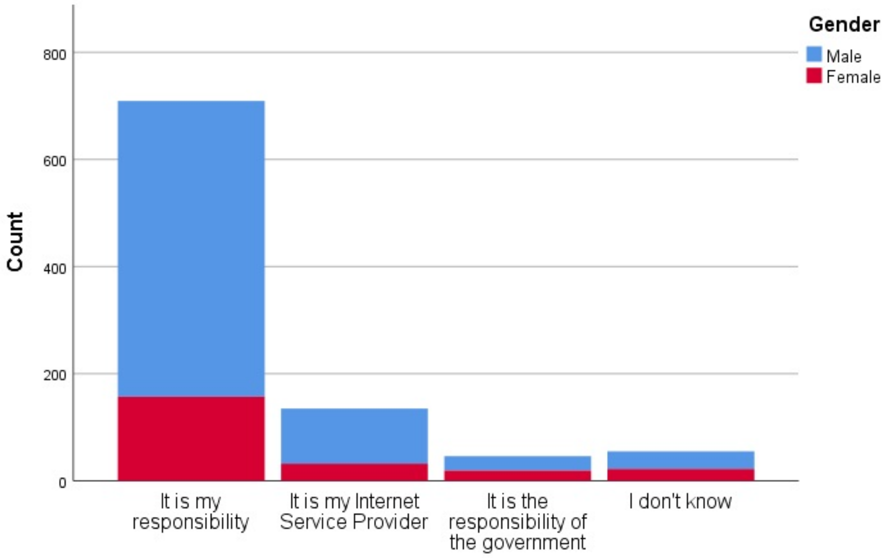


Figure 55: Who the users mean is responsible for their security, distributed by gender

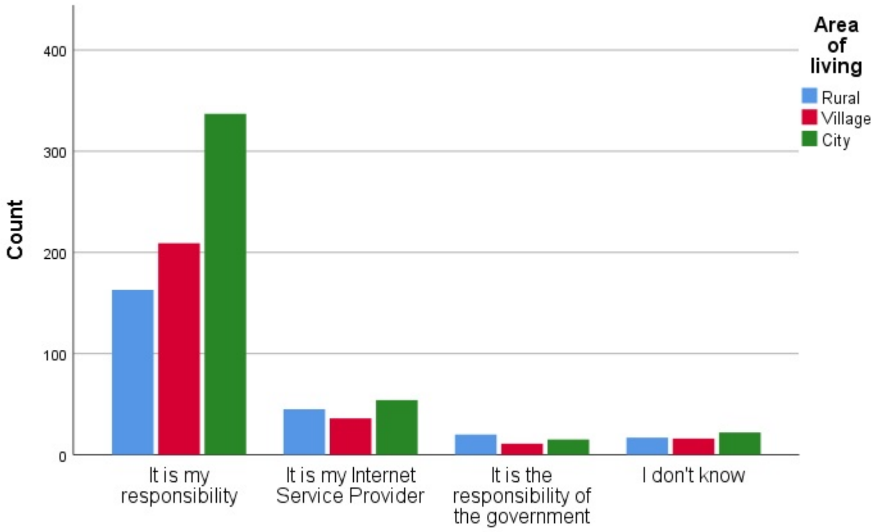


Figure 56: Who the users mean is responsible for their security, distributed by living area

The ANOVA test showed a variance within a small group of 4,9% that placed the responsibility on the government. For this group, there were 8,3% women and 3,8% men (Figure: 55).

65,5% of the people living in rural area place the responsibility on their selves, while 78,7% of the people living in the city answered similarly (Figure: 56). Placing the responsibility on themselves correlates with the users that are positive to ICT, have good knowledge and are aware of laws and regulations. However, the responses to the question didn't show any variations within the groups of education, age and employment factors.

Hence, it is reasonable to believe that a person with a raised level of security awareness, will place the responsibility of their security on themselves.

6.5.3 Freedom versus regulations

The question "I accept to have my activities online monitored if it makes me safer" intends to measure the level of privacy concerns in the population. 54,3% of the men and 59.1% of the women agreed or partly agreed to let their activities be monitored (Figure: 57). In respect of culture, this is a question that challenges the level of privacy toward how an individual relates to the level of unity in the Norwegian community. Hence, we implicitly asked if it is acceptable to give away privacy in return of safety.

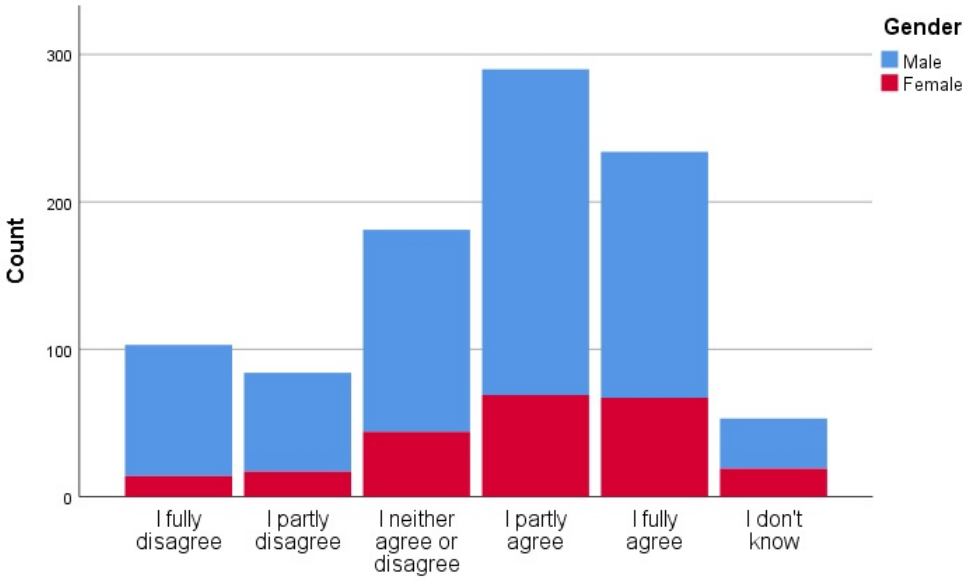


Figure 57: Level of agreement in having activities online monitored if it makes themselves safer, distributes by gender

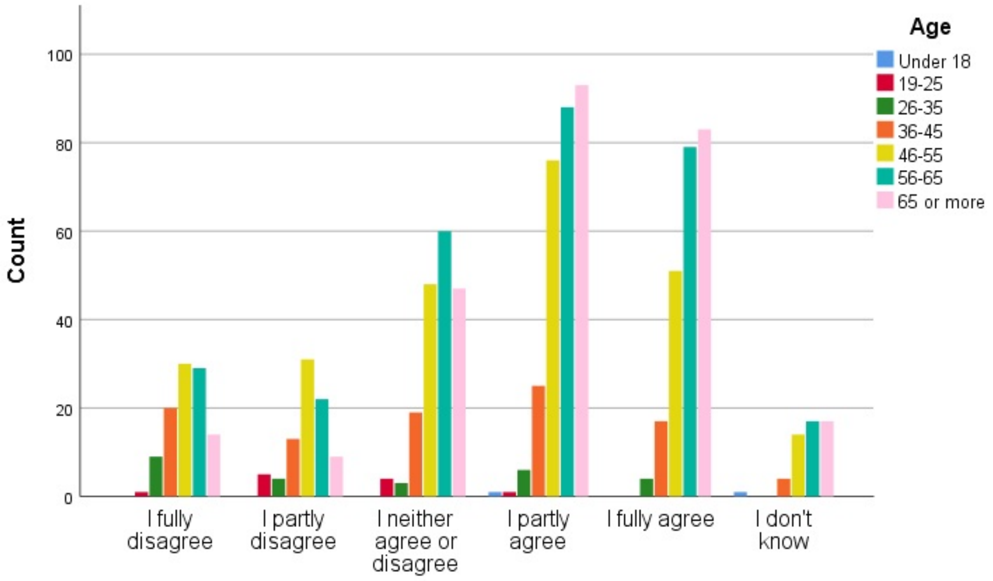


Figure 58: Level of agreement in having activities online monitored if it makes themselves safer, distributed by age

The ANOVA tests show that people over the age of 45 years deviate from the normal distribution. In particular, the elderly are very positive. Our sample of respondents has a high average age (Figure: 58), that means that the face-value is probably not very exact. The NorSiS survey ran in 2018 indicates that 59% do partly agreed or agreed to be monitored. This also slightly corresponds with our result. However, among the oldest people in the community of Eidsiva bredbaånd, they strongly deviate from the normal distribution. The reason for this is not known, but two hypotheses are that: 1 - It is correlated with knowledge or 2 - That the younger generations are more individualized the elderly. It is not identified any other groups that are more positive than others, except from the "working group" consisting of retired people (Figure: 59) that, of course, correlates with age.

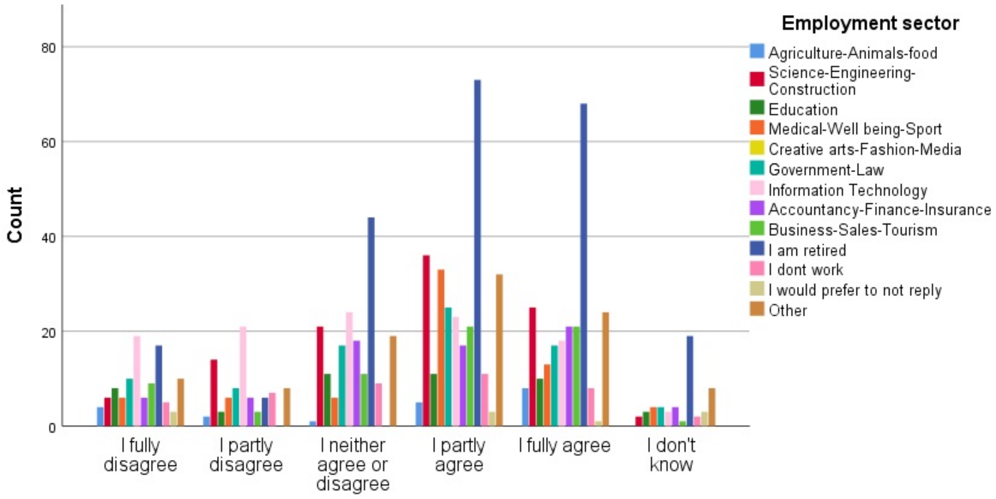


Figure 59: Level of agreement of having activities online monitored if it makes themselves safer, distributed by employmentsector

The majority of the users partly or fully agreed to have their activities monitored in order to be safer. However, 10,5% strictly disagreed with that. These people were also the most positive and considered themselves to have a high level of knowledge about online threats. This indicates that it is a correlation between being very concerned about privacy and having the knowledge about online threats.

6.5.4 Influence by regulations

In Section 6.3.4, we asked the users if they knew any national regulations or laws related to cyber security, where about half of the population agreed to that. This indicated a relatively low level of knowledge about laws and regulations, but we saw a clear indication that the people that work are more informed. We here zoom in on this question and ask about whether the people that work are aware of any cyber security regulations within their work of school environment. In this context, we do not seek to measure the level of knowledge, but we want to measure if active security control and training from companies have an effect on the security awareness of the users.

We filtered out all people that answered that they are retired or don't work. Then, 81,4% of this group replied "Yes" to know about any regulations. With respect to age, the only groups that were deviating from the overall result, were the users that were below 25 years (67,7% said "Yes") and the people above 65 years (53,7% said "Yes"). There was also a significant difference between the users in the city (87,5% said "Yes") and the users living in the rural areas (71,1%). However, we know from before that living area correlates with education, where we also here see a strong connection to both the level of education and the living area. The more education, the more "Yes" answers. For primary school education, 40,9% answered "Yes", while users with a Masters degree had 90,5% "Yes" replies and for the users with a Doctorate degree, 93,5% replied that they knew about any cyber security regulations at work (Figure: 60).

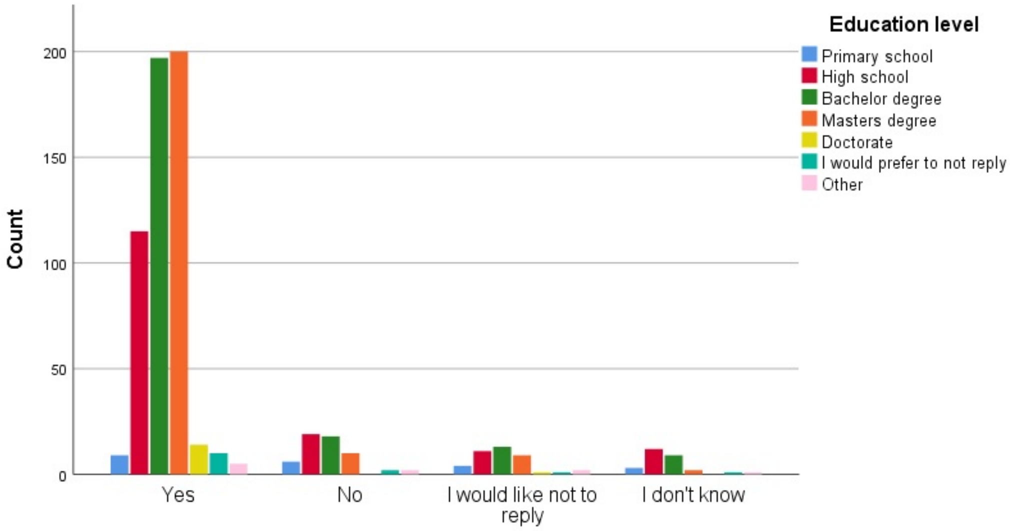


Figure 60: If their school or workplace have any rules or regulations about cyber security, distributed by educational level

We also see a variance between the different working sectors (Figure: 61). Among the users working with agriculture, 45,0% had heard about any cyber security regulations at work. The highest score was for the users who work in the government or with the law, where 95,1% replied "Yes". Secondly, the ICT sector and the Finance/Insurance sector were well informed, where respectively 89,5% and 88,9% from these groups answered "Yes".

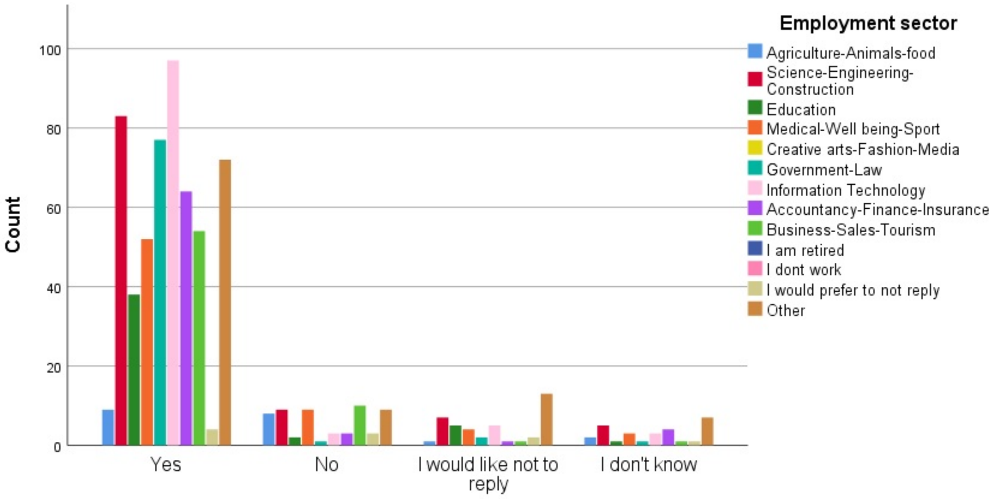


Figure 61: If their school or workplace have any rules or regulations about cyber security, distributed by employment sector

Our assumption about educational resources in big companies was also confirmed, where 92,0% of the employees in big companies claimed to be informed about any cyber security regulations. In medium companies, 79,2% answered "Yes", while only 65,6% of the users working in small companies replied "Yes".

Filtering out the users who don't work and the retired people, also resulted in a strong correlation with the previous questions. The people with high interest, high self-evaluated knowledge, and a great trust to the governments are over-represented in knowing about the regulations. Also, the question correlates with the amount of security training that is discussed in the next section.

6.5.5 Summary of trust

From this section, we have seen that knowledge affects privacy and trust in authorities. When the self-evaluated level of knowledge is high, then the threshold for reporting security incidents is lower and these users also tend to keep a higher personal privacy policy. This may also have a connection to the fact that among the people that work, they also have a high interest in ICT and have a high level of knowledge. They also have a high trust to authorities and they do know more about security laws and regulations than others.

We have also seen that if the users have a higher security awareness, they put more security responsibility on themselves. Another observation we have shown, is the importance of knowledge in order to be more aware of the cyber security threats, that indicates the general need for more training. How to let the national population gain more knowledge by training is discussed in the next section.

6.6 Education and training

It is identified that the self-evaluated level of knowledge is higher among the sample of subscription owners from Eidsiva than the general population in Norway. These users also claim to have a high level of trust towards authorities and self-evaluate themselves to have over average skills in evaluating risks. It is not known if this is caused by regional differences or if it is an attribute to subscription owners in general. However, it is expected that training in cyber security is a contributing factor to these high scores. Hence, it is important to identify the attributes of the users that have made them more security aware. Additionally, it is of high relevance how this sample has trained and if they would start or continues training. This section also aims to identify how trained they are, their training interest, how they would like to train and their stance towards training in cyber security. We also want to identify if there are any groups that would respond positively to customized cyber security training. Such questions about if and how the users want to train in cyber security, are not covered in the NorSIS report.

6.6.1 Acceptance of cyber security training

We asked the users: "On a scale from 1 (not important) to 6 (very important), how important do you think it is to educate people in information security?". With this question, we aimed to discover the users' general stance towards cyber security training. The results showed that 92,0% replied that they considered cyber security education very important (5 or 6) (Figure: 62).

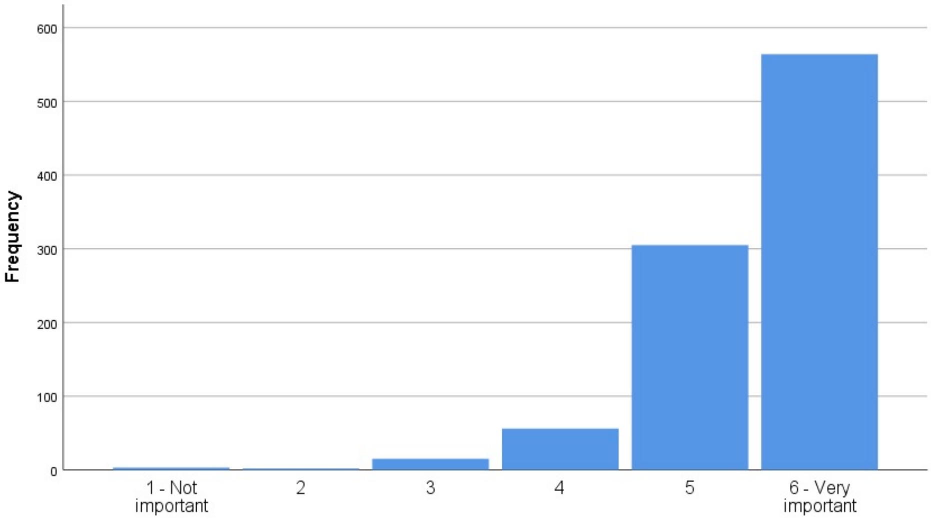


Figure 62: How important users think it is to educate people in information security

This result correlated with the users' general stance towards cyber security in Section 6.2.1. Hence, this is an indication that providers, such as Eidsiva bredbånd, should consider providing training programs for their users.

We have no other studies to compare this result with, but we consider it as a significant indication that security training is generally accepted among the population. We did not find any variations within any groups for this question. Hence, any group that did not agree with the importance of information security is not discovered. However, we take into account that based on the setup and headline of this survey, where the topic is "cyber security", potentially can influence the replies and the type of respondents.

Based on this positive response alone, we consider the general security awareness to be high. However, we do not know if the users know about the actual threats, but we do know, that most people acknowledge that it is important that the population has a cyber security awareness. On the other hand, we do not know why this awareness is high for the subscription owners of Eidsiva. We have discovered that they have a generally high level of self-evaluated knowledge and that their a perception of risks evaluations scored better than the rest of the Norwegian population. These attributes of knowledge and risk correlate with this positiveness of training.

6.6.2 Recent cyber security training

We asked the recipients of the survey if they had received formal cyber security training within the past two years. The hypothesis behind this question was that cyber security training has an effect on security awareness and perception of knowledge. This means that we can compare this question to the general security awareness questions, their current perception of knowledge and their willingness to receive more training. The face-value of the replies showed that 81,5% had not received any training, 17,5% had received training, while 1,1% preferred not to reply. This means that our sample has received less training than the sample NorSIS presented in their report, where 23% replied that they had received cyber security training and 71% claimed they had not. In the data-set, it was a clear skewness between the different groups related to age and working environment. Since less than 2% of the retired people answered "Yes" to have received any cyber security training, we filtered them out and performed the Bayesian ANOVA correlation test toward the demographic attribute of working environments. The test results showed that people working in large companies have received more cyber security training than others (Figure: 65).

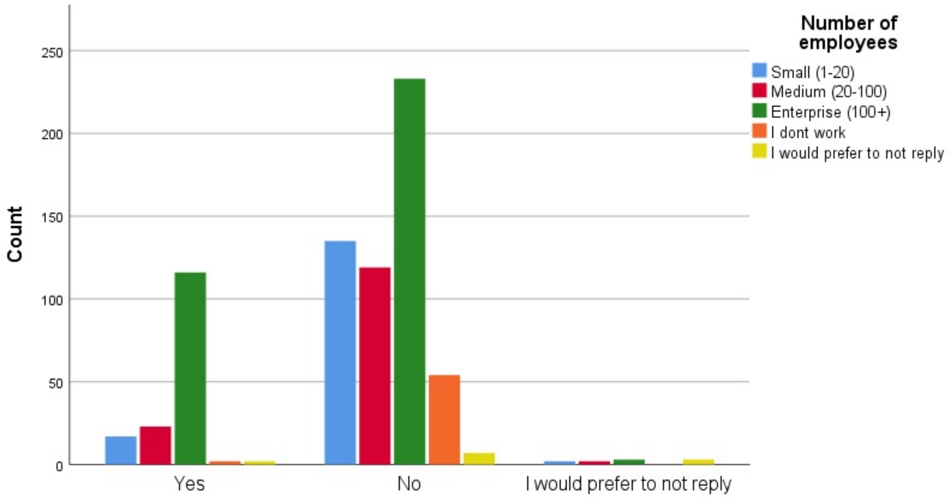


Figure 63: If the users have received any cyber security training, distributed by company size

The other two groups that deviate from the normal distribution is age and working sector. Out of the people working, there is a week indication that people between 36 and 55 years receive more cyber security training than others (Figure: 64).

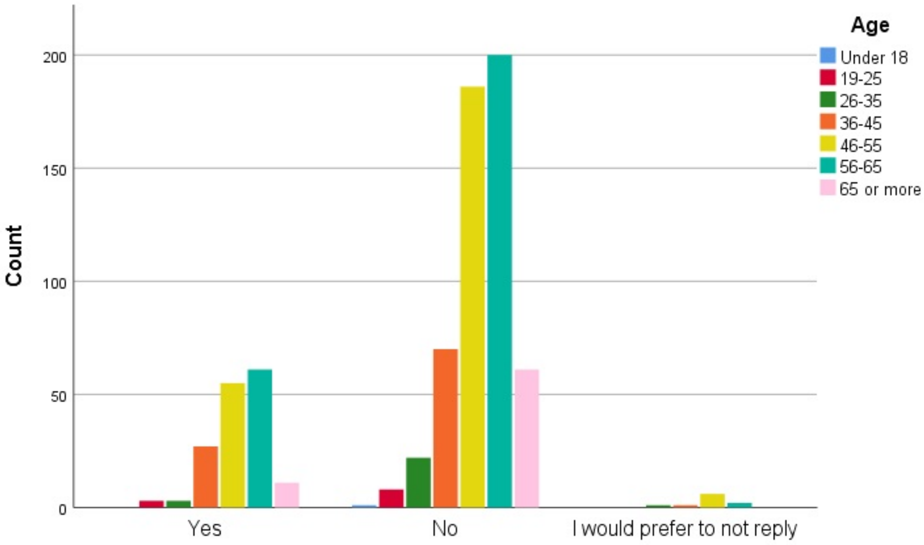


Figure 64: If the users have received any cyber security training, distributed by age

In respect of the working sector, the Bayesian ANOVA test shows that the working sectors of agriculture, sales and tourism receives the least amount of training, while the ICT sector gives the most training (Figure: 65).

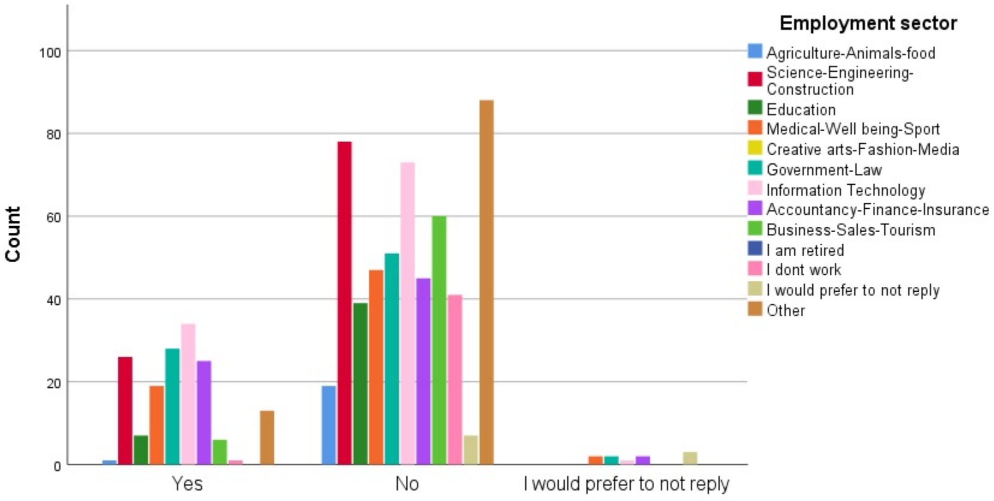


Figure 65: If the users have received any cyber security training, distributed by employment sector

This result does not confirm that the subscription owners of Eidsiva have more knowledge due to cyber security training. However, it does show that people working, especially in big companies, receives much more training than the people that are retired or are unemployed. This confirms our hypothesis.

6.6.3 Training methods

As we have seen in section 6.4, the level of knowledge is connected to the perceptions of risks. We have therefore also previously stated that security training is important in order to be aware of the security threats. NorSIS claims that it is the responsibility for both the government, the service providers and the individuals to provide the population with more cyber security knowledge. As a service provider, it is in Eidsiva's interest train their customers in order to protect both their customers and their network. Here, we aim to investigate from whom the customers would like to receive such training. In particular, we want to measure how the customers perceive the role of an Internet Service Provider as their training partner. Hence we asked the users: "How do you want to learn about cyber security?". For this question, we gave the users multiple choice alternatives in order to let them choose not only one, but multiple methods.

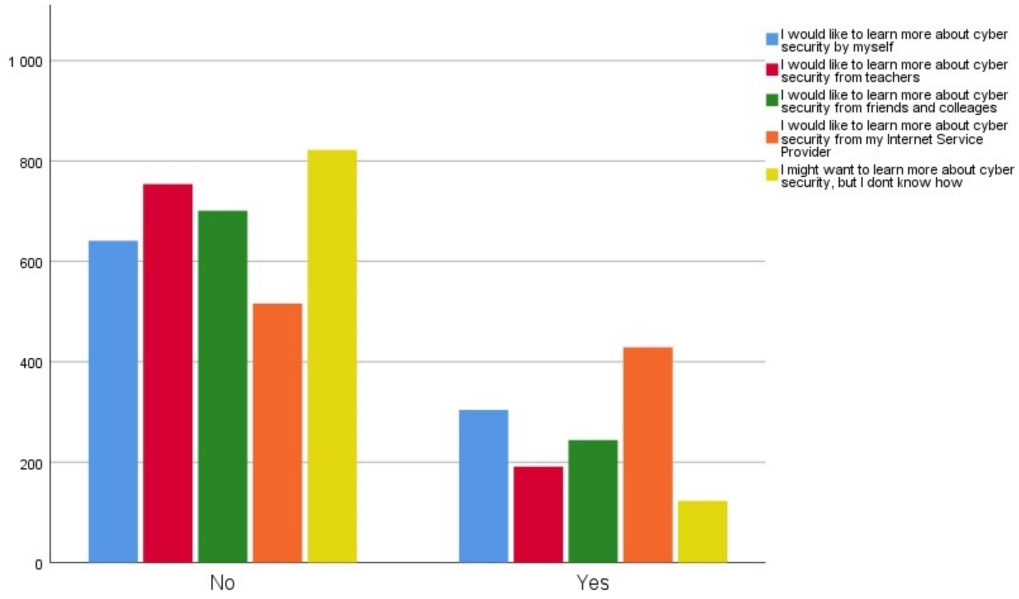


Figure 66: How the users want to learn about cyber security

Figure 66 shows that 32,3% of the users in the sample want to learn about cyber security by themselves, 20,2% wants to learn from teachers, 25,8% wants to learn from friends and colleagues, 45,4% wants to learn from their service provider while 13,0% answered that they did not know or that they did not want to learn. Between the alternatives, we found two relations. We found that the users that want to be taught from their service provider, tend to not want to be taught by teachers (76,0%) and they also don't want be learn by themselves (85,8%). Vica Versa, from the users that want to learn by themselves, 34,0% did not want to be taught by their Internet Service Providers (Figure:67).

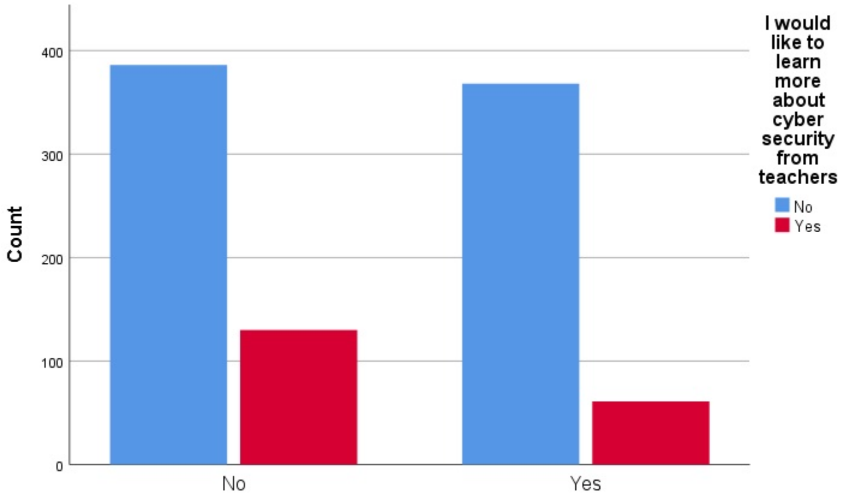


Figure 67: If the users would like to learn more about cyber security from their Internet Service Provider, distributed by those who want to learn from teachers

With respect to the demographic groups, the greatest variations we found for how the users that want to learn is age. We see a clear tendency that the older users get, the less they want to learn by themselves or from classroom teachers (Figure: 68).

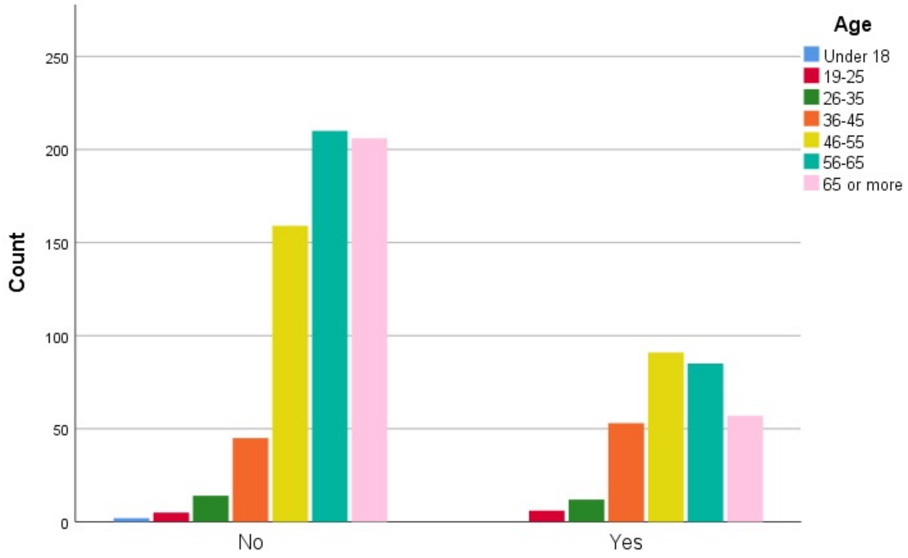


Figure 68: The users that would like to learn more about cyber security by themselves, distributed by age

However the elderly neither want to be taught by teachers. The resistance towards teachers increases for each age group, where 82,5% of the people above 65 would not like to be taught by teachers in a classroom. A similar increasing tendency for each age group is seen for being taught by friends, family or colleagues. For people under 25 years, 53,8% of them would like to learn from friends, family or colleagues. Among people above 65 years, 77,9% of them would not like to learn from their friends, family or colleagues. The opposite effect is seen when it comes to being taught from the Internet Service Provider, where there is a split between the age of 35 years. 34,6% of the people below 35 years would like to be taught from their Internet Service Provider, compared to 56,2% of the people above the age of 36 that would prefer such training (Figure: 69).

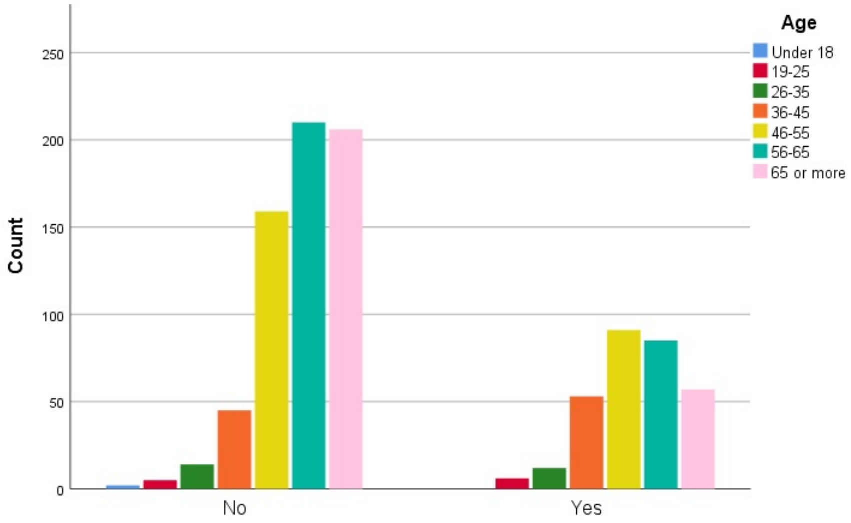


Figure 69: The users that would like to learn more about cyber security from their Internet Service Provider, distributed by age

Other groups such as gender and educational level did only variate for the learning methods of self-teaching. It is identified that men (Figure: 70) and users with higher educations primarily want to learn by themselves.

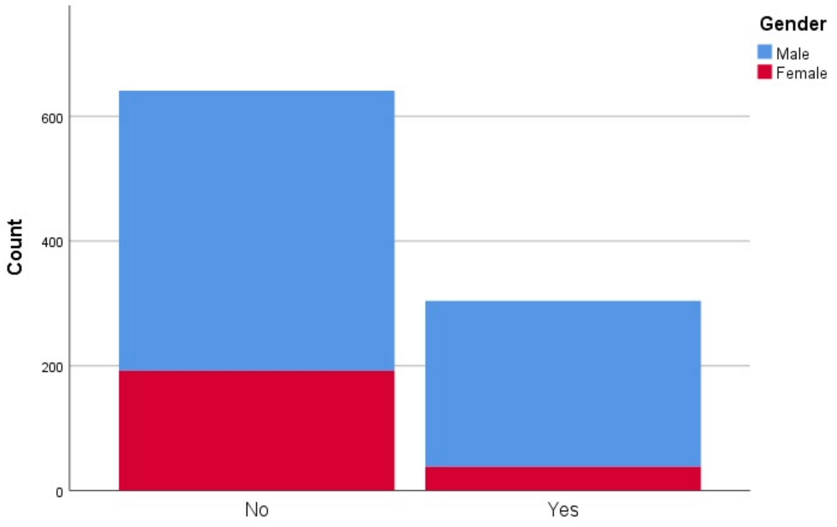


Figure 70: The users that would like to learn more about cyber security by themselves, distributed by gender

Figure 71 shows that around 20% of the users with primary school or high school educations would prefer to teach themselves, while 42,4% of the users with a Masters degree have a similar opinion.

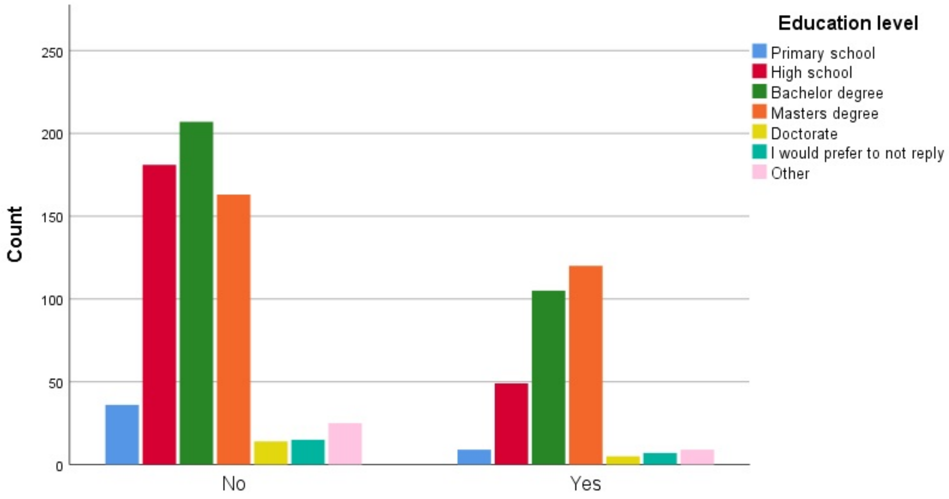


Figure 71: The users that would like to learn more about cyber security by themselves, distributed by educational level

From an Internet Service Provider perspective, the results gave primarily one indication of what group that it is beneficial for them working towards. We see that the older generations prefer that the Internet Service Providers are teaching them about cyber security. Based on the high average age of Eidsiva's subscription owners, it is recommendable that they run security training programs towards the older generations in particular.

6.6.4 Training preferences

Compared to the previous question, where we asked from whom the training was the most interesting to get, we here focus on how they would like to receive training. For this next question, we did not give multiple options, but we simply asked: "If you were to receive training on basic information security principles, would you prefer that in the form of: Self-study, Information emails, Online courses, Formal studies or lectures at work or school?"

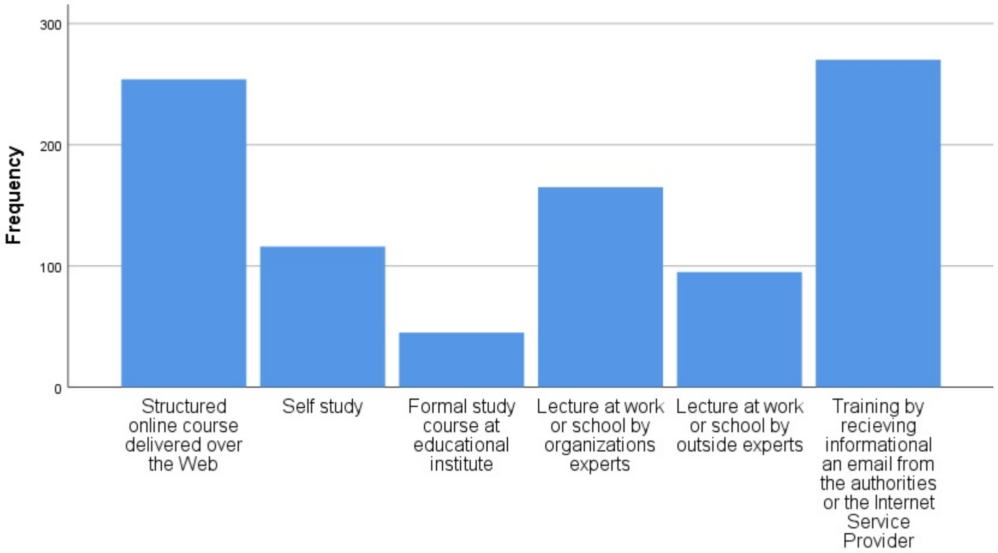


Figure 72: From whom the users would prefer to receive training about on basic information security principles

Figure 62 shows that the replies differ from the previous question. When the users are asked to prefer, only 12,3% would prefer self-study, while 32,3% were open to self-study as an alternative in the previous question. In the previous question, 45,4% replied that they would like their Internet Service Provider to provide training, while for this question, only 28,6% would like to receive an informational security message from their Internet Service Provider as the preferred option. This could also indicate that some of the customers also would like their Internet Service Provider to teach them about cyber security in other ways than information emails. 26,9% preferred online courses, 4,8% preferred formal studies and 27,6% preferred lectures at work or school.

Within the different groups, there is a difference between men and women, where 29,1% of the men and 20,0% of the women prefer web-courses. The opposite distribution is seen for letting the Internet Service Provider send cyber security informational letters, where 26,3% of the men and 35,7% of the women prefer this option (Figure: 73).

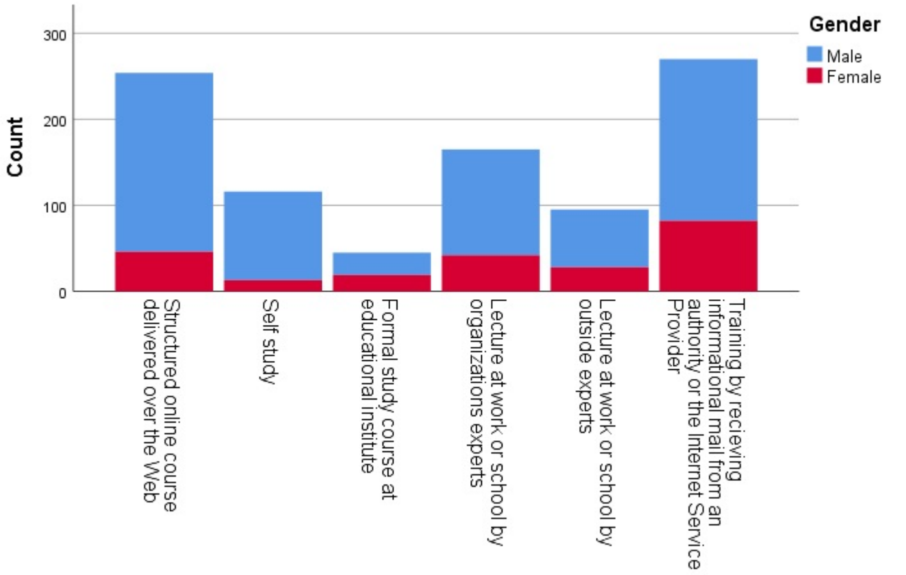


Figure 73: From whom the users would prefer to receive training about on basic information security principles, distributed by gender

The preferred option of cyber security training also differs between the age groups (Figure: 74).

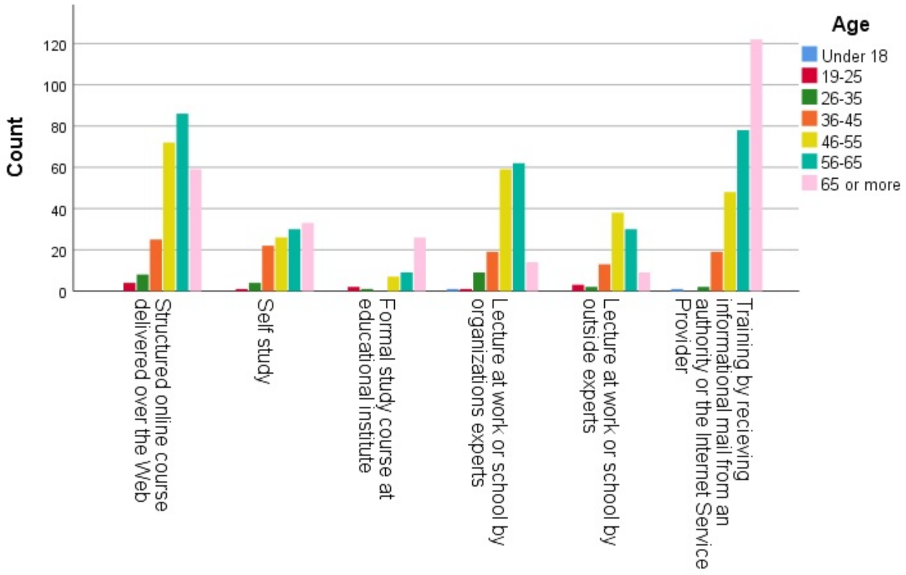


Figure 74: From whom the users would prefer to receive training about on basic information security principles, distributed by age

There are not any options that clearly sticks out, but it is a significant trend that the older generation (above 65 years) wants to have informational emails more than the other groups. Also, for all other age groups, 28,6% preferred structured online courses. If we filter out all the people that don't work, we did not find any change in the distribution for the people below 65. However, among the people that work, 36,4% of them want to receive training at work by internal or external experts.

From an Internet Service Provider perspective, the results show that 55,5% of their customers would prefer to receive training by informational emails or structured online courses.

6.6.5 Distributing knowledge about cyber security

The previous questions about cyber security training indicated that over half the customers of Eidsiva bredbånd would prefer to let their Internet Service Provider take responsibility for training them in cyber security. This confirms what we expected, therefore, we also asked a more direct question. We asked: "Would you sign up in a free of charge security awareness campaign, where you periodically receive informative material on best practices and recent threats?"

The results showed that 82,2% were positive such information. However, we see a similar difference between the age groups as we saw in the previous question about cyber security training (Section: 6.6.2). The level of interest increases by age. 57,7% of the people in the age group 26-35 years replied "Yes", while 92,4% answered "Yes" in the age group of 65+ years (Figure: 75).

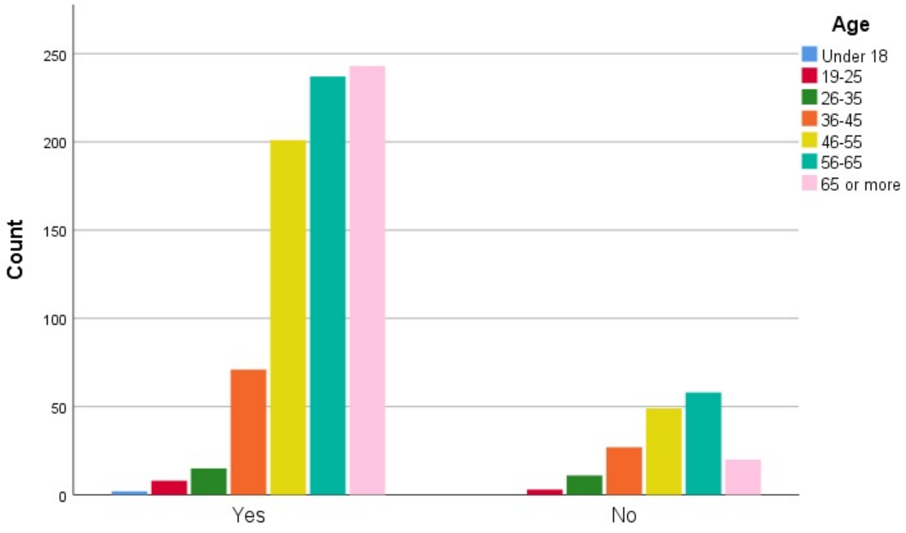


Figure 75: If the users would like to sign up for a free-of-charge cyber security awareness campaign, distributed by age

For the other demographic attributes, it was only one group that deviated from distribution. The users that were working in big companies were more negative to such information than others. 83,0% of the users in small companies said "Yes", while 76,2% said "Yes" among the users working in big companies. We do not know the reason for this, but one hypothesis is that the users working in big companies might already receive a large amount of such information by for example their email at work. Hence, they might not value even more emails of such information. This theory is based on our previous result that showed that this group of people has more knowledge and receives more training than the other groups that are working in smaller companies.

6.6.6 Amount of security training

Since the users are interested in receiving cyber security training, it is important to scale the number of training events to an acceptable level. If a customer receives too much training emails or courses, there is a risk that the users lose interest. Therefore we asked the users: "How much time per month are you willing to dedicate on security awareness training?"

In fact, 79,8% of the users were willing to spend 15 minutes on more on security training per month. We also found a similar variation within the age group for this question. For example, for the age groups 25-45 years, 30,8% of them were willing to spend more than 30 minutes on security training. 43,2% of the age groups 46-65 years and 52,2% for the group 65+ years, agreed to spend more than 30 minutes per month on security training (Figure: 76).

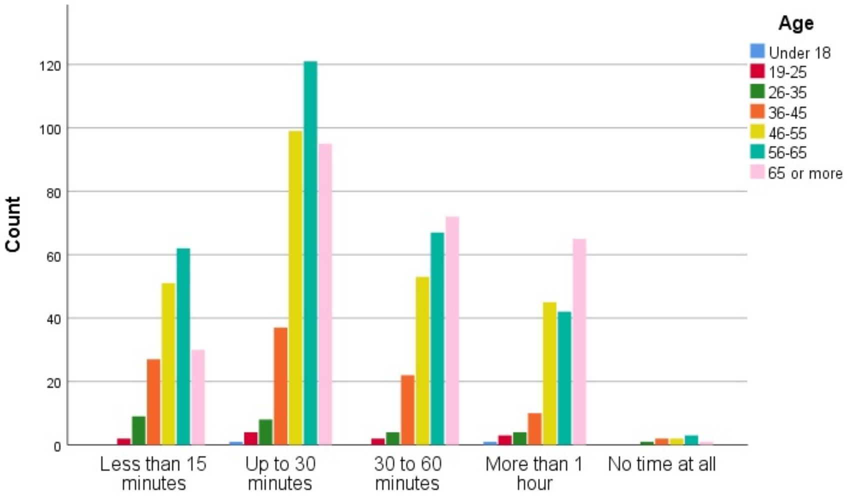


Figure 76: The amount of security training the users would like to receive, distributed by age

Not surprisingly, we also identified that the users that do not work are willing to spend more time on cyber security training than the users that work. No other demographic groups deviated from the normal distribution.

6.6.7 Summary of education and training

We have identified that the sample of subscription owners of Eidsiva bredbånd are very positive towards cyber security training. However, the user sample has in fact received much less cyber security than the rest of the Norwegian population. Hence, the high level of self-evaluated knowledge is not explained by cyber security training.

We have identified that people working in big companies have received more training than people in small companies. Also, it is identified that people that are retired or unemployed have received less training.

There is a difference between the age groups in both from whom, how and how much training they are willing to receive. The older generations are more interested in informational emails, younger people are more interested in structured online courses and the people that work would prefer to get their training at work. It is also identified that the people that do not work are willing to spend more time on cyber security training than the people that work.

However, a key finding is that a majority of the users want their Internet Service Provider to run security training programs towards them. Based our the results, a training duration of 15 to 30 minutes per month is preferable.

6.7 Cyber security behavioural patterns

As mentioned in Section 6.3, the self-evaluation of knowledge we measured earlier is high subjective. Hence, we also want to compare their self-evaluations in the previous questions toward their cyber security skills and behaviour through a set of basic cyber security principles. We refer to this as an analysis of cyber security behavioural patterns. Due to the number of available questions that are reasonable to have in a survey, we limited the questions to only concern WiFi connection, authentication, authorization, backup and online behaviour.

6.7.1 WiFi connections

Security awareness also includes being aware of basic network connections. We expect that not everyone knows the difference between cabled, WiFi and 3G/4G Internet connections. However, if they know what a WiFi network is, it is important that they are aware of the potential risks in connecting to such networks. Their main concern should be that there could be fake or malign access points and that their wireless network traffic can eavesdrop. This applies to both mobile phones and computers, where the general advice is to use known networks with the latest password encryption method. We asked the user three questions about WiFi connection. We asked if they connect to free WiFi with mobile phones and Computers in order to measure how aware they are about malicious access points or the awareness of the network they connect to. We also asked about their awareness of encrypted WiFi connections.

36 users (3,8%) connected to any wireless network with their mobile phone without any concerns, while 21 users (2,2%) connected to any wireless network with their laptop without any concern. On the other side of the scale, is the people that do not connect these WiFi networks at all. For this group, we do not know if not connecting is because of their lack of need, their lack of capability of connecting or because of their security and privacy awareness. Here, 14,7% never connect WiFi with their mobile phones and 24,1% never connect to WiFi with their laptop. However, the threat relies within those who connect to any network without any concerns. For the groups that 1 - connect to a network they choose to trust and 2 - the users that are careful about their actions when connected to a WiFi network, we here consider to be security aware. We consider our result as positive where it indicates that fixed lines internet subscriptions owners are generally aware of the risk of connecting to free WiFi.

In general, there is a slight difference between how the users perceive WiFi security on their mobile phones versus their laptops. It is not known if this is due to their usage patterns or if it is a perception of different levels of connection safety between mobile phones and laptops. With respect to demographic groups, we see a variance for two groups only; the area they are living in and the number of employees at their workplace. This applies to both mobile phones and laptop connections. For the living areas, we see that 22,9% of those who live in the rural areas never use WiFi on their mobile phones and 1,2% of those who live in the rural areas had no concerns about connecting their mobile phone to WiFi (Figure: 77).

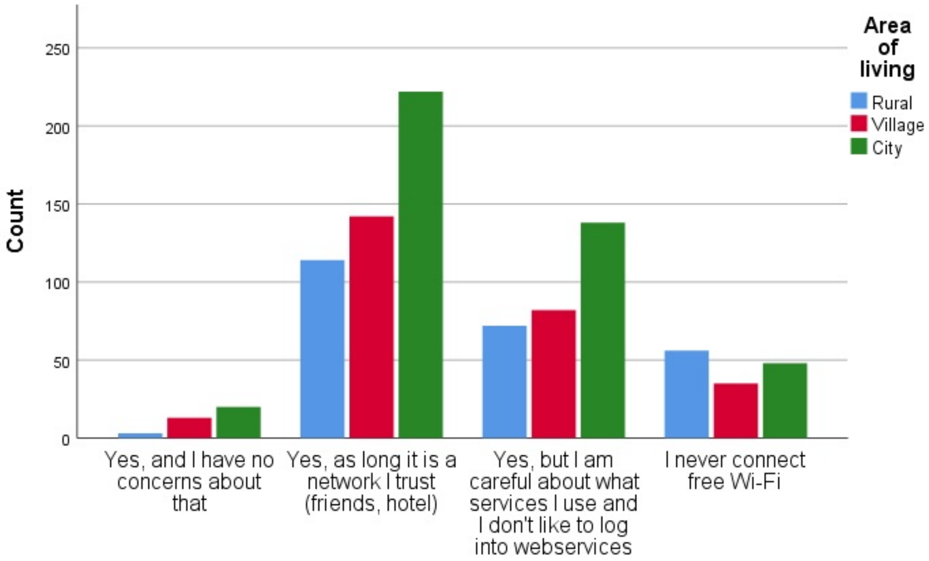


Figure 77: If users would connect their mobile device to free WiFi, distributed by living area

However, for connecting the laptop to free WiFi, the users in the rural areas are even more aware than the users in the city. 0,4% of the users in the rural areas had no concerns connecting, 31,0% never connects, while 68,6% are security aware when connecting to WiFi networks with their laptops. In comparison, 2,8% of the users in the city were not concerned about connecting their laptop to free WiFi (Figure: 78).

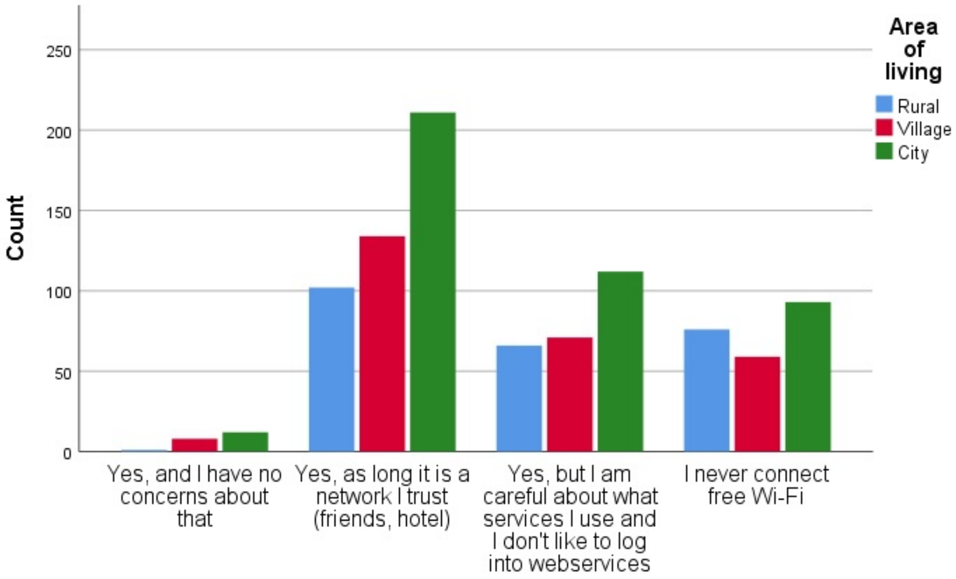


Figure 78: If users would connect their laptop to free WiFi, distributed by living area

This does not confirm our hypothesis that people in rural areas are less security aware, but it actually shows a slight indication of the opposite.

We found no other variations within the demographic groups, except that people that don’t work connect less to wireless networks for both mobile phones and laptops (29,5%).

The third question about wireless connections we asked the users about was: "Do you turn off password protection on your wireless connection?". The question is phrased in this way because it is reported from Eidsiva that all their customers get broadband routers delivered from them with password protected WiFi enabled.

82,2% of the respondents replied that they do not turn off this and 5,4% said that they did turn it off.The age group that most frequently turns their wireless passwords off, is the age groups of 36-55, where 7,5% of the users turn this off (Figure: 79).

With respect to employment sectors, we see that people working with Agriculture (15,0%) and ICT (7,4%) are also groups that frequently turn off WiFi encryption. The users that do not work or are retired, are the groups that most frequently do not turn off the WiFi password protection.

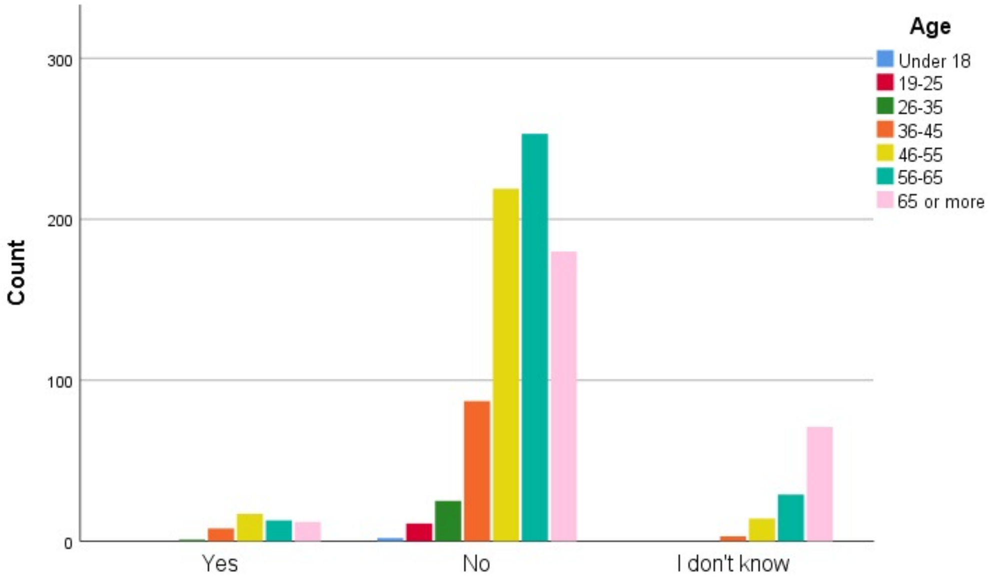


Figure 79: If users turn off password protection on their WiFi connections, distributed by age

6.7.2 Authentication

One of the most frequent security incidents is when an attacker gets access to the username and password of a victim. Typically an online service or a computer get compromised and an attacker gets access to one or multiple user accounts of different online sites. In order to secure ourselves against this, security measures such as two-factor authentication and the use of unique passwords among different online sites can reduce the consequences of a compromised password. However, using authentication protocols such as OpenID [20], open up for multiple websites to utilize a shared authentication service (i.e Facebook or Google). Then, the trust in the authentication service depends on how much the users trust the provider, where the level of trust also can be perceived as a level of security. In this section, we aim to investigate how aware the users are about protecting their user accounts from being compromised. Hence, we asked the users about how they log in to services and how they handle their passwords. First, we asked the users: "Which of these options do you use to authenticate your access to websites?"

We gave the users the opportunity to select multiple options, with a simple "Yes" or "No" answer. Figure 80 shows that 12,3% replied that they use their Facebook account to log into other websites, while 20,7% used their Google account for the same purpose. 43,5% answered that they prefer to create a separate login for each web account they establish and 44,8% replied that they choose to use two-factor authentication when available. Only 5,4% did not understand the question.

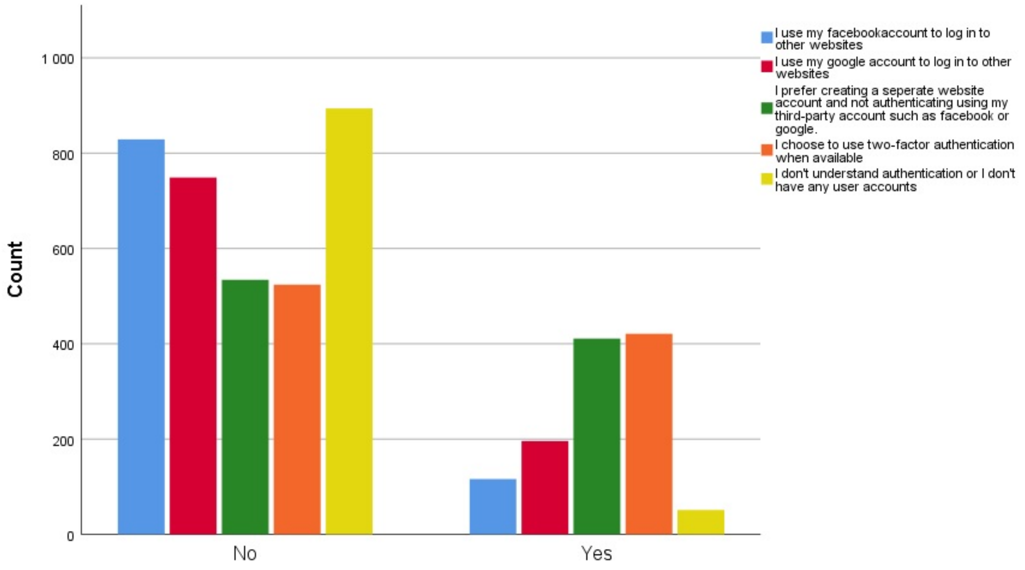


Figure 80: Which options the users use to authenticate themselves towards websites

25,9% of the users that used a Google account, also used a Facebook account. Only 7,1% of the users that used Facebook as an authentication service for multiple web accounts, also used two-factor authentication. Similarly, 11,6% chose to use two-factor together with the Google accounts. On the other hand, for those who primarily preferred to create a separate account for logging into websites, 29,9% of that subgroup also chose to use two-factor authentication when available. We interpreted the result as, in general, people that preferred to create their separate account password instead of using OpenID, consider that more secure. This is based on the fact that most of them chose to use two-factor authentication and therefore they are more security aware. We see a pattern in the demographic groups of what authentication service that is the most in use among the groups. 47,7% of the men and 34,8% of the women chose to use two-factor authentication when available (Figure: 81). However, gender does not variate for the other authentication options chosen.

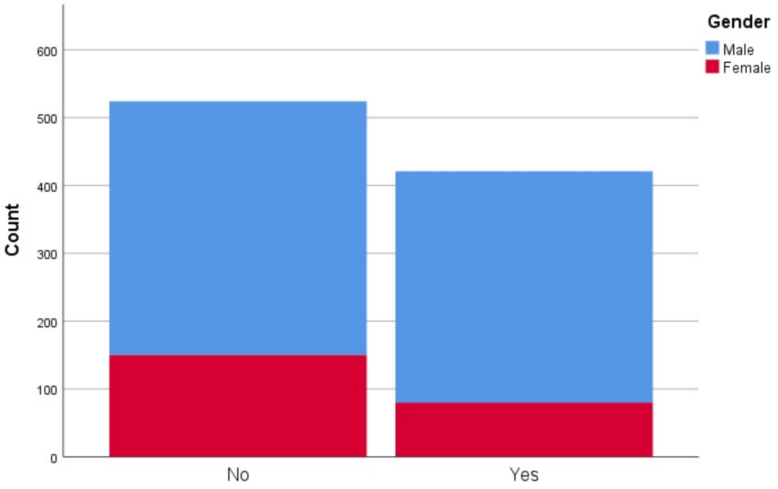


Figure 81: If users choose to use two-factor authentication when available, distributed by gender

Regarding age, there is a clear indication that the use of both OpenID and preferring using a separate account, decrease by increased age. 9,5% of the users above 65 use Facebook to log into other websites, compared with 24,1% among people below 35 years. 81.8% of the users below 25 years chose to create separate user-names and passwords for different websites, while only 28,5% of the users above 65 years replied that (Figure: 82).

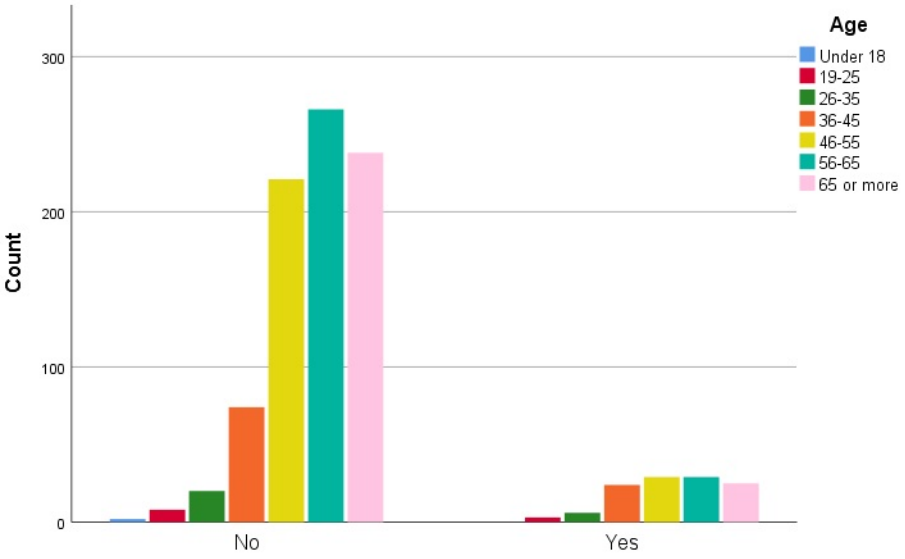


Figure 82: If users use their Facebook account to log in to other websites, distributed by age

It is also noticed that especially the older generations have denied using all alternatives. They have also denied that they don't understand or that they don't use. This indicates that they have accounts on the web they log into, but there is a missing alternative for them. In retrospect, we realized that we had not taken other OpenID vendors into the alternatives, such as the Norwegian authentication method of using the BankID system. However, BankID authentication is not what we wanted to measure, but we wanted to measure how the users create accounts and passwords for different websites. That 27,1% have denied every alternative, is therefore a valid result, that indicates that they do not use the authentication method that we wanted to measure. Among the users that did not understand the question, 62,7% of them had an educational level of primary school or high school.

We found another interesting fact, that for people working in big companies, 53,3% of them chose to use two-factor authentication when available. This, compared to the people working in small companies, where 40,3% chose to use two-factor authentication (Figure: 83).

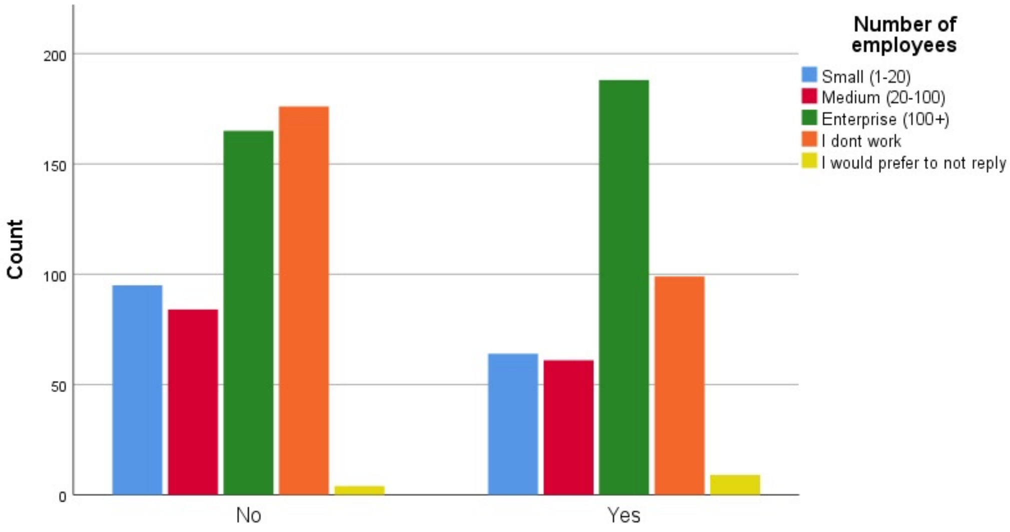


Figure 83: Users who chose to use two-factor authentication when available, distributed by the number of employees

As mentioned when introducing this subsection, another factor that describes the security awareness behaviour, is how the users create their passwords. Hence, we asked: "What characterizes the passwords that you use?" Most people are aware of creating different passwords for different websites. 50,1% of the users in our sample use a slight variation of the same passwords, while 45,3% intend to use different passwords for different sites (Figure: 84). In retrospect, we realized that we did not discover the level of variance in the passwords. If the passwords vary with for example only a digit at the end of the password, then it is not considered a good variation. However, variations that are not easily detected are considered good. Hence, the results are considered inconclusive, but positive. Our results also comply with the NorSIS report from 2018, where 44% replied that they intend to use different passwords for different websites. We did not find any variation within the different groups for this question.

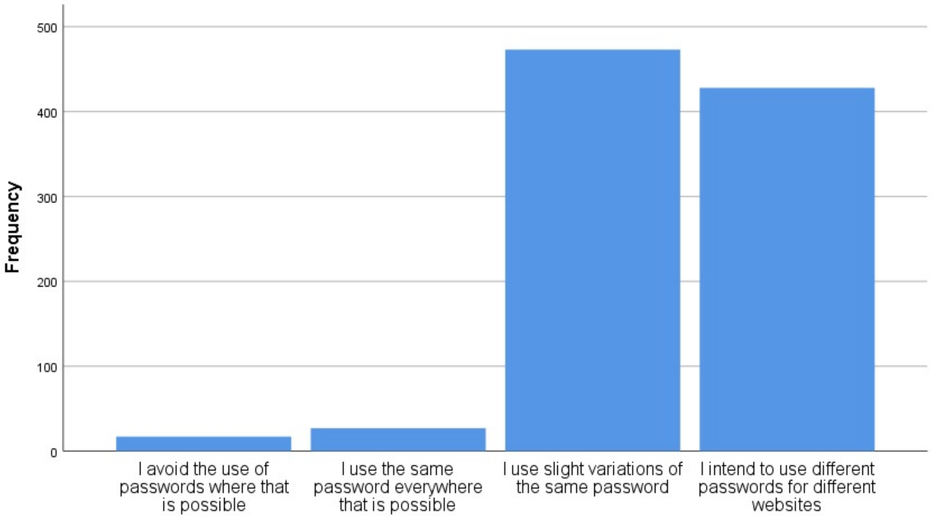


Figure 84: Characterizations of the users' passwords

Another aspect of passwords is how we can remember them. Since it is generally recommended to use many different passwords, it is difficult to remember them all. Therefore, people use different remembering methods that are associated with different security levels. Their method is a behavioural pattern connected with security awareness. We asked the users: "Which method do you use in order to remember your passwords?"

Figure 85 shows that different people use many different methods for remembering them. The different methods they used are not identified as significantly special for any group in our survey. All demographic attributes such as age groups, gender, education and work are equally distributed among the methods. Neither are any of the alternatives considered to be very wrong if the context is correct. However, NorSIS recommends using tools such as password-managers, but only 12,7% if the users used such a tool.

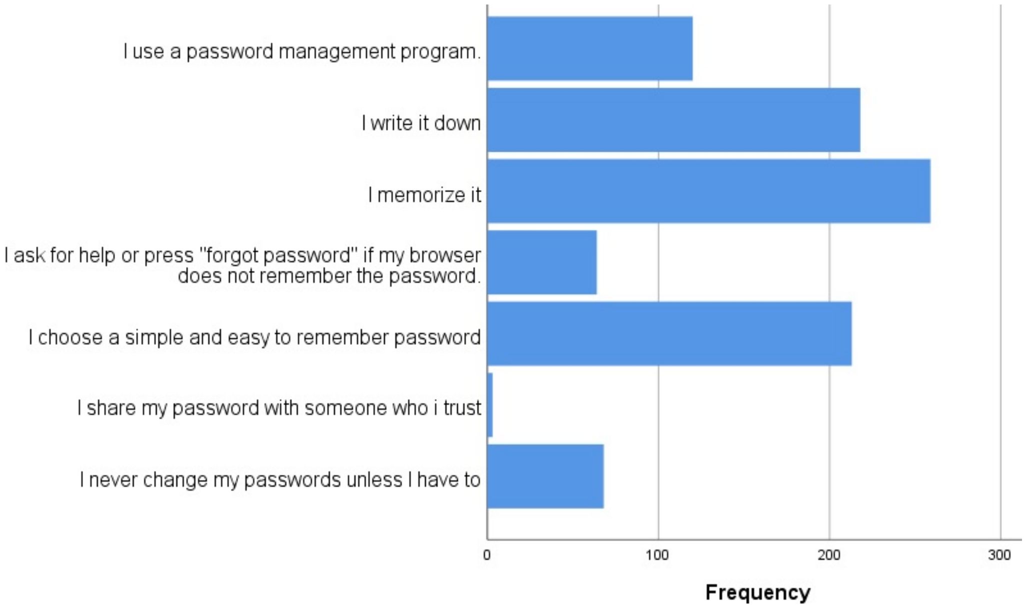


Figure 85: Password remembering methods

In general, our results authentication were inconclusive in identifying any connections between remembering passwords, password characterization and authentication methods. As a general reflection and example of the topic, sharing your unique Netflix credentials with your wife or husband, is different than announcing your password on social media. Hence, the subjectiveness of these questions is high, where the contexts of the reply options are difficult to discover.

6.7.3 Authorization

It is understandable that not everyone reads terms and conditions when installing a program. On the other hand, for mobile devices in particular, it has become easier for end-users to understand what access level an application requires in order to be installed. However, it is assumed that some users often feel forced to install these applications. We assume that some people do install some of these applications, despite their privacy concerns. We wanted to measure the level of privacy concern and awareness of these installations. However, it is difficult to measure how the users prioritize the need for using an application versus their privacy concerns. Our assumption is that most users have attempted to install an application that is not considered "needed" at least once. If one of these "optional" application is seen to violate our privacy, then we assume that the users have an awareness and a level of concern about their privacy. Therefore, we asked the users: "How frequently do you check the permissions (access rights) that the application requires before completing the installation?" 79,3% of the users have declined to install an application more than once. 14,0% said they have never done that and 6,8% did not understand the question (Figure: 86).

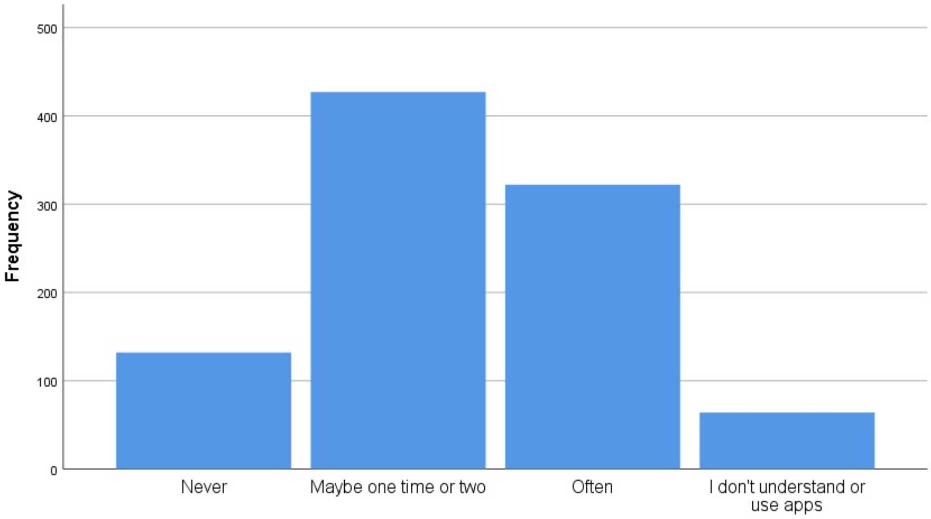


Figure 86: How frequently the users check the permissions (access rights) that the application requires before completing the installation

We did not find any correlation to our demographic attributes, but the question correlates with the general risk evaluation questions. For example; How worried the users are in general, how worried they are for connecting to WiFi and how worried they are using online services. If you are worried (level 5 or 6) about the security on your mobile device (Section: 6.4.6), then 81,4% of these users also decline application installations due to their privacy concerns.

6.7.4 Backup

We had a hypothesis that application synchronizations to cloud services have made the general population less concerned about backups and that we rely more on the cloud services now than before. Hence, traditional backup no longer has the focus as it had a decade ago for many users. In order to confirm the hypothesis we asked the users: "How do you take backup?"

Figure 87 shows the distribution of the different backup methods among the users. 57,6% of them use a backup disk service in the cloud, 14,7% use a cloud-based backup program, 44,9% take local backup periodically and 10,8% use a local network storage device. However, the most interesting result is that 10,1% do not use backup and 3,1% do not know if their data is backed up.

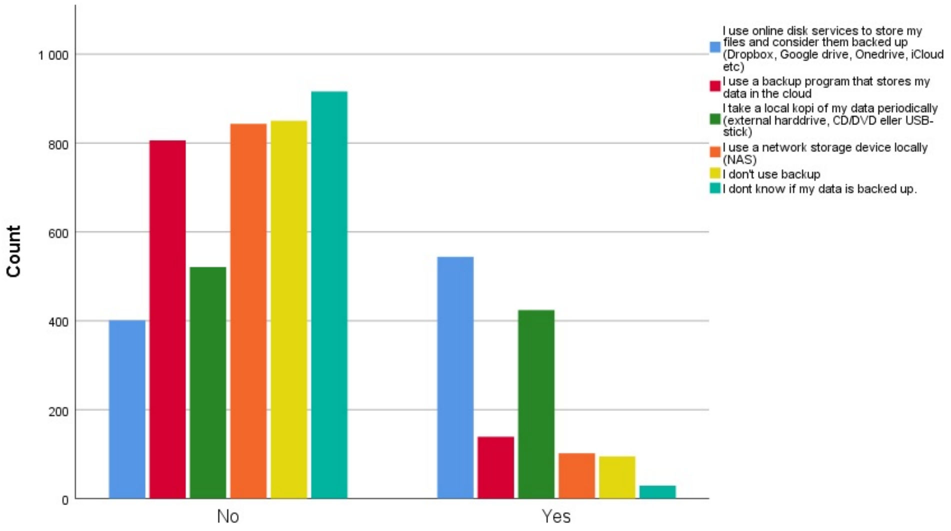


Figure 87: Which options the users use to take backup of their data

For the users that did not use backups, we found variations within the groups of age, living area, employment status. The deviating groups are the users that do not work or are retired. Within the age groups (Figure: 88), the retired people they take less backup than the other age groups (20,3% do not take backup). Also, among the users who do not work, but are not retired, they are also taking less backups (16,7% do not take backup).

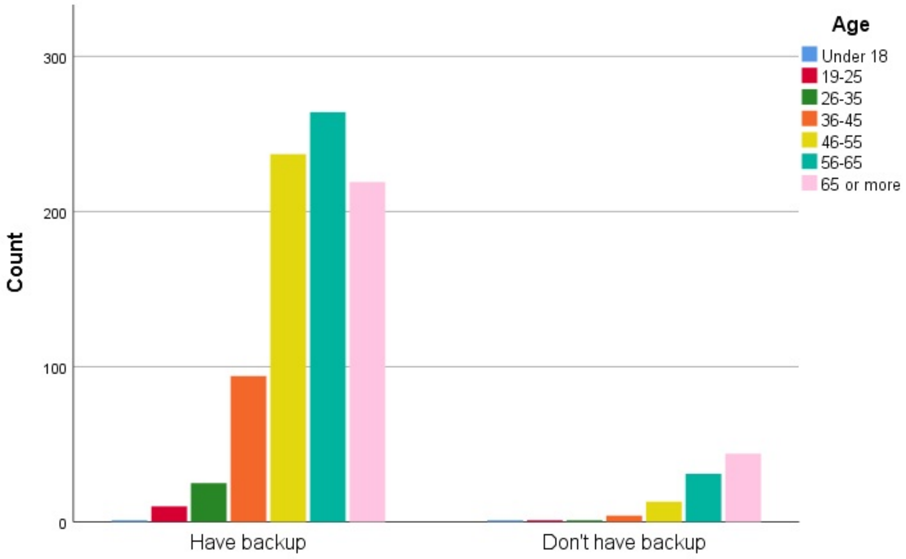


Figure 88: The users that don't have backups, distributed by age

For the other age groups, we see no significant variations.

Interestingly, the users in the rural area do neither take backups as much as the users in the other areas. 17,6% of the users in the rural areas, 9,2% in the villages and 6,3% of the users in the cities do not take backups.

For the users that do not take backups, we see a connection to their level of interest, their knowledge, their risk evaluations and to the users that would have a self-study education. For example, 98,3% of the users that are very interested in ICT also take backups. Regarding the knowledge level, 99,6% of the users that consider themselves to know more the average population, also take backups. A similar connection is also seen to awareness of laws and regulations.

There is a significant connection between the users that are very worried and among those who take backups. For example, only 13,8% of the users that don't back up are not worried or a bit worried about being manipulated (Figure: 89).

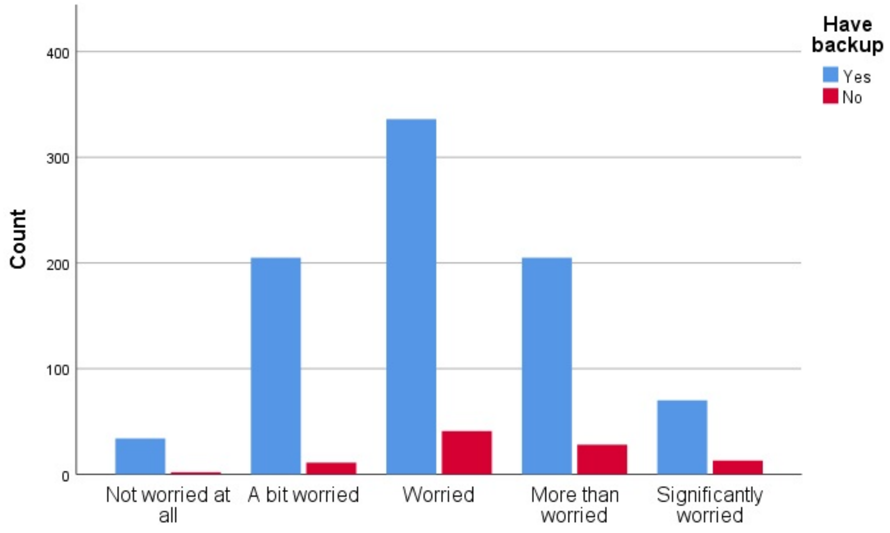


Figure 89: How worried are you about that you will be manipulated to send sensitive information to someone compared to those who chose not to take backup

The correlations confirm that being worried have necessarily nothing to do with being aware of the threats. We suspect that the level of being worried can consist of two reasons. 1 - That some users are both aware and afraid of the threat and 2 - that they are generally worried because they do not know about the threats. Being worried because of the lack of control or the lack of knowledge is also a type of a security awareness, but it shows that our measurements of risk evaluations are not necessarily based on the awareness of the threats. Hence, it is not possible to conclude that the users with high interest, knowledge and not being worried, have a higher security awareness because they take backups. It is possible that some users simply don't have anything to take backup of. However, we assume that the combination of being worried because of a lack of control or because of a lack of knowledge, is an element that is mostly distributed among the oldest generation.

Another interesting result is that 57,5% consider cloud services such as Google Drive as a sufficient backup. We do not know if they are using i.e. the Google drive as a secondary storage device for backups or if they are using it as their primary disk without any additional backup. If they are using it as their primary disk, we assume they consider that disk drive as backed up by the cloud provider. We assume some users perceive such cloud services as a general protection of hardware failure on their personal device. What the users are not fully protected against in such cases, are for example deletion of files. We cannot identify this difference of awareness based on our questions. However, based on the fact that this question about cloud disk services correlated towards 40% of all the other questions in the survey, we see a connection of using such services with the level of security awareness. 50,5% of the users using cloud disk services also have an additional local backup. However, it is not known how many of them that use the disk as their primary disk without a local backup, because they perceive the cloud as securely backed up. Also, we do not know how many users that use a local disk as their primary disk and use a cloud disk as a backup disk.

An age group that in particular deviated from the normal distribution for this "cloud disk" question is the 24-35 age group. 80,8% of the users in this group used cloud-based disk-services as their backup service, while the older age groups have decreasing use of that. Only 42,2% of the oldest generations are using cloud-based disks as a backup service (Figure: 90).

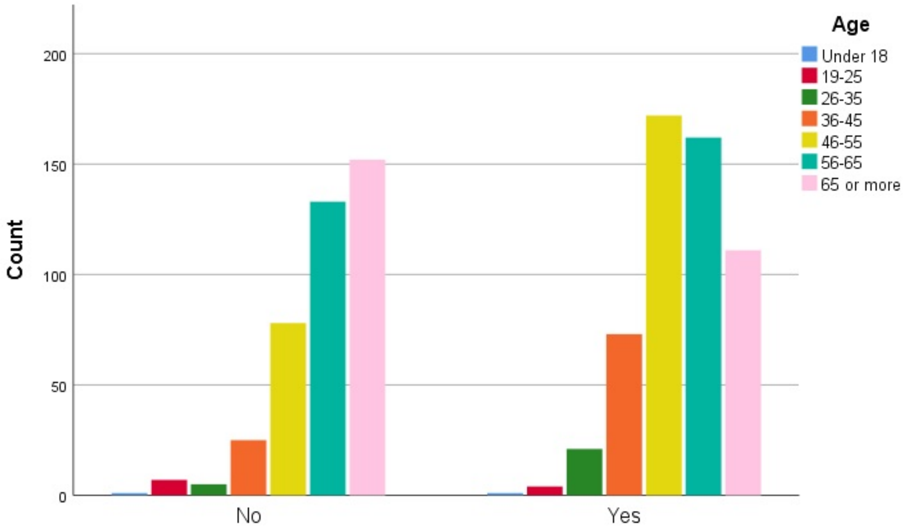


Figure 90: The users who use online disk services to store their files and consider them as backed up, distributed by age

48,8% of the users in the city used cloud-based disks versus a use of 63,8% in the cities. We also see an increased use of cloud-based disks with an increasing education level. Contrary, there is a low-level use of cloud-based disks among the retired people (40,5%) and those who don't work (40,1%). There were no indications of variance with the groups of the number of employees and the employment sectors for these questions.

6.7.5 Phishing awareness

Phishing is one of the most known cyber security attacks [7] that for some users also are associated with spam. It is assumed that most people are aware of the existence of non-legitimate emails, but the finesse in some of the phishing emails can make them difficult to detect. Hence, we measured the behavioural patterns of the users in our sample by asking them the following: "When receiving an e-mail that appears to be coming from your bank and asking you to go to a specific web link to confirm your personal details, what would you do?"

Figure 91 shows that most users have an awareness of phishing. We categorized the options of contacting the bank or ignore the request as highly aware, and the other options as not being aware. The result shows that 93,7% of the respondents handle this with being security aware.

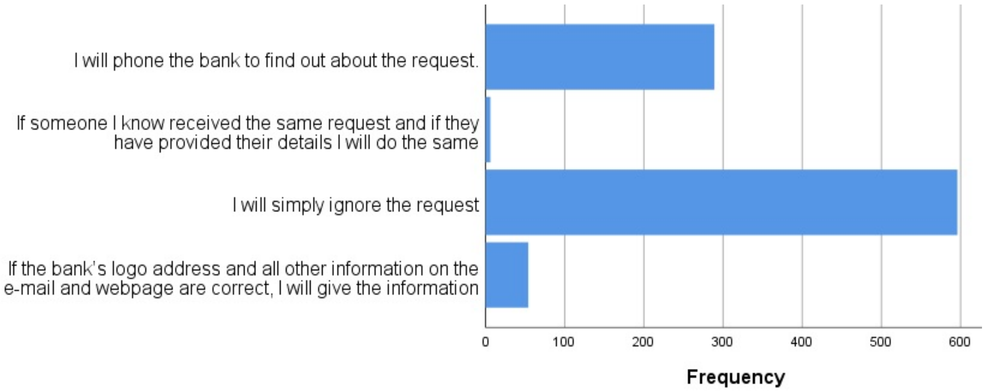


Figure 91: The actions taken when receiving an e-mail that appears to be coming from your bank and asking about personal information

More interestingly is the other group that is in fact considering providing such information. 13,5% of the users below the age of 35 would provide such information. This decreases for every age group where 4,1% of the users in the age group 56-65 would provide such information. However, the oldest age group does not follow the linear pattern of decreased use by age, where 7,2% of the users above 65 years claim to provide such information (Figure: 92).

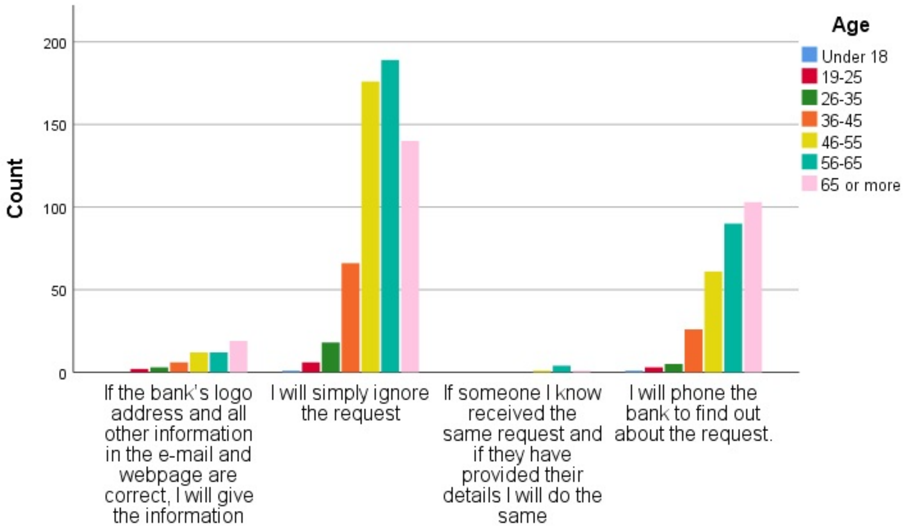


Figure 92: The actions taken when receiving an e-mail that appears to be coming from your bank and asking about personal information, distributed by age

Another interesting observation is that the users that work in medium-sized companies have a higher rate in providing such information than the other company groups. 10,4% of the people working in medium-sized companies would provide the information, while 5,2% of the employees in bigger and smaller companies answered similarly.

6.7.6 Summary of the behavioural analysis

In this section, we discussed the behavioural pattern within cyber security. We confirmed that the users that have the interest and the knowledge also behave more securely. However, we discovered that being worried do not necessarily result in a secure behaviour. We assume that there are two ways of being worried: Worried about the unknown because of a lack of knowledge and worried about the threat because of the knowledge about it. We also showed that our hypothesis about the users in the rural areas are less security aware, is likely to be false. The users in the rural areas connect less to free WiFI than others. However, we saw that the users that don't work also connect less to free WiFi, that indicates that this result can also be caused by less access to WiFi networks in the rural areas.

Another interesting observation is that we found three groups that are less concerned about their WiFi privacy than others. The age group of 36-55 years, the people working with ICT and the people working with agriculture are the largest groups of users that choose to turn off the password protection of their WiFi connections.

We asked three questions about authentication and passwords. By correlating the replies to the question about two-factor authentication, knowledge and interest, we saw that the users consider it more secure to create a separate web-account with a separate user-names and passwords instead of using a centralized authentication service such as OpenID. However, we also saw that a large group, especially of those with lower education, did not understand the authentication concept. Another interesting finding was that people working in large companies chose to use two-factor authentication more frequently than others. This confirmed our hypotheses that bigger companies have more resources to educate their employees than the smaller companies.

Analyzing how the users were aware of creating and handling their passwords were inconclusive, where we did not find any unique characteristics for any groups.

We found that the level of security awareness during installation of applications gives an overall indication of the level of security awareness. 79,3% of the users declined to install an application more than once. However, we did not find any attributes that characterized this group.

For the use of backup, we saw that retired persons and the users that do not work take less backup than the other groups. However, we do not know if this is because they do not know how, if they are not aware of it or if they basically do not have any data worth backing up. We did identify that the level of being worried depends on the level of knowledge. However, the measurements of how worried the users are, do not necessarily correspond with having a high cyber security awareness.

Regarding phishing, there seems to be a general awareness of the problem, but surprisingly, it is the age group of the users below 35 years that has the lowest thresholds of giving away their personal information in phishing attacks. Also, the people that work in medium size companies, in particular, are willing to provide such information more frequently. Based on our correlation tests, we assume that this is because they trust their own skills in evaluating what is safe or not safe. However, such e-mails that appear to be coming from banks are highly suspect. That the younger users with high self-evaluated skill are willing to give away such personal information, witness that they have trust in their own knowledge and evaluation skills. However, this also shows that they are willing to take bigger risks.

7 Conclusion

One of the objectives of this survey was to establish a collaboration with the industry and find a common area of interest with academia. Security awareness among the Norwegian population is targeted as a problem from both NorSiS and the industry. We consider that sending out the survey by itself, contributed to a higher security awareness among the customers of Eidsiva bredbånd.

The results of our study indicate that the level of security awareness within the Norwegian society can be significantly improved. The main objective of this article was to identify focus areas for such future studies, in order to highlight methods towards increasing the security awareness of the general public. Our results indicate that, even if people consider themselves slightly above average aware, in terms of security awareness, this perception does not always match their actual knowledge and behaviour. This is a similar conclusion to what NorSIS presented in their report from 2018. However, we have identified that their questions should have more nuance to them. They are generally stating that a wider and stronger knowledge base is needed across the nation, but they do not explain how and why. We identified that usage patterns, knowledge and the level of being worried are highly subjective. We have seen that general cyber security awareness relies highly on individual perceptions, and that training, consequently, must be customized for the different groups.

The survey was distributed to approximately 10000 of the subscription owner of Eidsiva bredbånd with fixed internet connection lines. The sample consisted of an over-representation of men and elderly people. However, this does represent the general distribution of age and gender for fixed-line internet subscription owners in general. Based on correlation tests in the SPSS tool, we have taken this skewness into account and evaluated our result based on statistical correlation tests for comparison with other studies.

We have seen that a security awareness study towards internet subscription owners of Eidsiva bredbånd gave different results in contrast to other national studies. The sample of internet subscription owners that we analyzed, has generally a better understanding of cyber security than other data-sets. This is particularly interesting in order to identify the attributes in the data, that can make us raise the general security awareness. However, we did not find a general explanation for the result, except that the data-set consists of internet subscription owners. But, we did identify groups such as gender age, living area, education and employment attributes in the data-set, that can be used to customize cyber security training.

Our data sample consisted of a group of highly positive users towards cyber security compared to other studies, but their general interest in ICT was lower than the user sample in the latest NorSIS report from 2018. We saw that the general interest in both information security and technology affects the level of security awareness and knowledge. By comparing the interest towards behavioural patterns, we saw that increased interest and positiveness, result in a better cyber security awareness. However, with a response rate of around 10%, it is not known if the respondents who chose the answer the survey, had more interest or were more positive towards security or ICT than among those who did not reply.

When measuring knowledge by self-evaluation, we noticed the subjectiveness of the questions. However, by correlating the questions towards the knowledge tests, security behaviour and risk evaluations, we saw a variation between knowledge perception and actual knowledge. The subscription owners of Eidsiva bredbånd rate themselves as above average knowledgeable. For example, 90,1% claims to be aware of online threats, while only 65% knows about any security regulations. These opposites confirm the subjectiveness of these surveys in general.

With respect to risk evaluation, we discovered that the users in our data sample were much less worried than the rest of the national population. We saw that these users also had a high level of trust towards authorities and that they had a generally high level of self-evaluated knowledge. This confirms the assumption that gaining knowledge increases trust in both service providers and authorities. It also confirmed, that gaining knowledge are making us lower the threshold of what we consider as risks. The paradox is that more knowledge makes us take bigger risks, but it also makes us more security aware. This means that when working with security awareness training, it is equally important to work towards the users with high knowledge, as it is towards the users with less knowledge. That increased confidence in skills makes us take bigger risks, we particularly noticed for the age group of 36-55 years and for the users working with ICT. This pattern was especially seen for WiFI security. We also discovered that people below 35 years have a lower security awareness regarding phishing.

Our study shows that the behavioural pattern among the different groups vary and it is closely connected with what services they use. For example, an old woman, with less skills, that uses her computer for online banking and reading email only, can have a good security awareness of these two services. Based on her use, she can have a satisfying security awareness compared to a person that has a much wider use of services. However, their perception of feeling safe differs if we ask for a specific service or asking them generally. The older generations are generally more worried, but when asking about specific services they use, they are not as worried as others. We defined that as two types of being worried. Worried about the unknown and worried about a certain threat. One example of this, we also found when analyzing behavioural pattern for backup. Some people do not have anything they value as important to backup and therefore they do not need backup. Hence, not taking backup does not make them less security aware.

We have also seen that the level of knowledge affects the users' general stance towards privacy. A high level of knowledge makes the users take more responsibility for their own safety. However, there is a difference in the general stance towards privacy and the behavioural patterns concerning privacy. It is identified that people below 35 years are more willing to provide their personal information than the older generations, as we have discovered while asking about phishing.

Both NorSIS, our results and the service providers emphasise the importance of cyber security knowledge and training. Subscription owners of Eidsiva bredbånd are, in particular, more interested in training than the rest of the population in Norway. However, based on the low amount of training the users have received, it does not explain why the level of knowledge is high. It is identified that the need for training among the population is very individual and that the industry already provides training. This is especially seen for people working in big companies. For people that are unemployed, retired or working with agriculture or tourism, the need for training is not fully covered. These groups have also agreed to spend more time on training than the other groups. Most importantly, they also tend to prefer that their Internet Service Provider provides such training. The older generations want informational emails, while the younger generations want structured online web courses.

Our hypothesis that people working in big companies have more security training and therefore are more security aware, was proven to be true. This also indicates that this group of people does not need that much training focus from an Internet Service Provider perspective. Analyzing the behavioural patterns within cyber security, we identified that people in the rural areas are more worried and also act more securely, by not connecting very frequently to free WiFi. This proved the opposite of our hypothesis and showed that the users in the rural areas are in fact more security aware than the users in other areas.

Finally, the indicators show that many users that perceive themselves aware of the security risks, still do not follow the general security recommendations under specific circumstances. For further security awareness studies, we suggest to identify the factors that raise the security awareness, and the reason behind not following existing security guidelines. We also suggest to further study people's perception of privacy and their willingness to take risks. In our future studies, we also intend to further investigate the difference of being worried because of having and not having the knowledge about the threats.

We also raise the question if there is a security parallel between driving cars and cyber security. Men consider themselves to have more interest in cars and being better drivers than women, but in fact, they are involved in more car accidents. There is a similar perception of the oldest generation, that they both have less skills in driving cars and handling ICT. Is it the case that women and the elderly in fact are involved in less cyber security incidents than the rest of the population? For future work and upcoming surveys, it is recommended the questions must be more nuanced in order to disclose this.

8 Acknowledgement

I want to thank my supervisors Dr Vasileios Gkioulos and Dr Gaute Wangen for helping me through the process of completing this survey. Risk assessment and surveys, in general, have been a new topic for me, where I learned about both new methods, tools and theories when handling our data-set. I also want to thank Eidsiva bredbånd for the collaboration and for providing us with both a sample of their customers and for providing us with a framework for managing the survey. An acknowledgement also goes to the marketing department in Eidsiva bredbånd consisting of Mona Ulimoen, Kim Thomas Sivertsen and Amund Hagejordet for helping us with correcting the Norwegian formulations of some of our questions.

Bibliography

[1] Barn og medier, medietilsynet, 2016.
ONLINE: http://www.medietilsynet.no/globalassets/dokumenter/trygg_bruk/fra-barn-og-medier-2016-digital-mobbing.pdf , Visited: 2018-12-13.

[2] Befolkningens utdanningsnivå, statistisk sentralbyrå, 2018.
ONLINE: https://www.ssb.no/utdanning/statistikker/utniv, Visited: 2018-12-13.

[3] Befolkningsprofil, statistisk sentralbyrå, 2018.
ONLINE: https://www.ssb.no/kommunefakta/kostra/oppland/befolkningsprofil, Visited: 2018-12-13.

[4] Davide Ariu, Francesca Bosco, Valeria Ferraris, Pierluigi Perri, Giovanna Spolti, Pasquale Stirparo, Giuseppe Vaciago, and Stefano Zanero. Security of the digital natives. *Available at SSRN 2442037*, 2014.

[5] Silja Baller, Soumitra Dutta, and Bruno Lanvin. The Global Information Technology Report 2016. Technical report, World Economic Forum, July 2016.

[6] W Scott Blackmer. Gdpr: getting ready for the new eu general data protection regulation. *Information Law Group, InfoLawGroup LLP, Retrieved*, 22(08):2016, 2016.

[7] Kang Leng Chiew, Kelvin Sheng Chek Yong, and Choon Lin Tan. A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 106:1 – 20, 2018.

[8] Vasileios Gkioulos, Gaute Wangen, Sokratis K Katsikas, George Kavallieratos, and Panayiotis Kotzanikolaou. Security awareness of the digital natives. *Information*, 8(2):42, 2017.

[9] Vasileios Gkioulos, Gaute Wangen, Sokratis K. Katsikas, George Kavallieratos, and Panayiotis Kotzanikolaou. Security Awareness of the Digital Natives. *Information - Information and Communications Technology, Special issue: "Mobile Systems, Mobile Networks and Mobile Cloud: Security, Privacy and Digital Forensics*, 8(2):42, 2017.

[10] Bilal Khan, Khaled S Alghathbar, Syed Irfan Nabi, and Muhammad Khurram Khan. Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5(26):10862–10868, 2011.

[11] Hennie Kruger, Lynette Drevin, and Tjaart Steyn. A vocabulary test to assess information security awareness", Information Management & Computer Security. *Information Management & Computer Security* , 18(5):316–327, 2010.

[12] Morten Levin and Roger Klev. *Forandring som praksis: læring og utvikling i organisasjoner*. Fagbokforl., 2002.

[13] Bjarte Malmedal and Hanne Eggen Røislien. The Norwegian Cyber Security Culture. Technical report, NORSIS - Norwegian Center for Information Security, 2016.

[14] Bjarte Malmedal and Hanne Eggen Røislien. The Norwegian Cyber Security Culture. Technical report, NORSIS - Norwegian Center for Information Security, 2018.

[15] Blaž Markelj and Igor Bernik. Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications*, 20:84–89, 2015.

[16] Blaž Markelj and Sabina Zgaga. Comprehension of cyber threats and their consequences in slovenia. *Computer Law & Security Review*, 32(3):513–525, 2016.

[17] Janne Merete Hagen, Eirik Albrechtsen, and Jan Hovden. Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4):377–397, 2008.

[18] Kathryn Parsons, Agata McCormac, Marcus Butavicius, and Lael Ferguson. Human factors and information security: individual, culture and security environment. Technical report, Defence Science and Technology, Edinburgh (Australia), 2010.

[19] Marc Prensky. Digital natives, digital immigrants part 1. *On the horizon*, 9(5):1–6, 2001.

[20] David Recordon and Drummond Reed. Openid 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*, pages 11–16. ACM, 2006.

[21] IBM SPSS et al. Ibm spss statistics for windows, version 20.0. *New York: IBM Corp*, 2011.

[22] S. Talib, N. L. Clarke, and S. M. Furnell. An analysis of information security awareness within home and work environments. In *2010 International Conference on Availability, Reliability and Security*, pages 196–203, Feb 2010.

[23] Ryan West. The psychology of security. *Communications of the ACM*, 51(4):34–40, 2008.

[24] Michael Workman, William H Bommer, and Detmar Straub. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, 24(6):2799–2816, 2008.