Cybersecurity Awareness and Culture in Rural Norway

H.Gunleifsen, V. Gkioulos, G. Wangen,
A. Shalaginov, M. Kianpour and M Abomhara

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway
e-mail:{hakon.gunleifsen2, vasileios.gkioulos, gaute.wangen, andrii.shalaginov, mazaher.kianpour, mohamed.abomhara}@ntnu.no

Abstract

Understanding the level of security awareness, perception, and culture of users in aspects related to security is crucial for the development of suitable and effective protection measures for both Internet users and the utilised infrastructure. This understanding becomes imperative in countries with increased integration of Information and Communication Technologies (ICT), such as Norway. In this paper, we present a summary of results from an extended study of the security awareness and cybersecurity culture of Norwegian users of ICT. Specifically, the study targets Internet subscription owners in rural Norway and identifies how their security awareness can be improved. The study was conducted using an online questionnaire which got 945 respondents. This study differs from previous measurements because it targets an older segment of the population (average age 56 years) which primarily resides in rural Norway. The paper presents results for the sample within the areas of general stance toward IT, knowledge, risk evaluations, and trust in authorities. Furthermore, we analyse the training preferences and compare their self-evaluated skills in knowledge and risk-evaluations with their actions and behaviour online. The results show that the level of security awareness is highly subjective and that training programs and security awareness campaigns are both needed and requested by end-users. We have concluded that a customised need for cybersecurity training among targeted groups of end-users.

Keywords

Security, Awareness, IT-knowledge, Cybersecurity, Training

1 Introduction

Internet access and omnipresent connectivity have become an indispensable part of our everyday life, fulfilling the increasing users' desire to access the 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 adversarial activities, such as identity theft, blackmailing, active data collection, malware infection or defamation (Peters et al., 2018). In light of this, it is important that users are aware of both the potential risks and the available trivial countermeasures.

Within such an emerging environment, a critical requirement towards safe and secure information society is to prepare people, aligned with contemporary societal needs, to encounter future challenges in their personal and professional life. The main challenges are related to our increasing dependency on digital technologies and the corresponding needs to improve cybersecurity awareness. Digitalisation is a key enabler of economic growth and welfare improvements for the Norwegian state, industry, and society at large (Malmedal et al., 2018). Yet, this study shows that cybersecurity 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 socio-technical one, which is highly influenced by human factors. As highlighted by earlier studies (Malmedal et al., 2018), (Gkioulos et al., 2017), the competence, awareness, and risk perception of users, are critical dimensions of cybersecurity. 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.

Through this study, we seek to identify critical Internet 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 cybersecurity awareness and readiness of the Norwegian society. Accordingly, we aim to study and analyse such socio-technical attributes as cybersecurity knowledge, risk assessments and behavioural analysis focusing on supporting the development of novel intervention actions, educational policies. Moreover, the idea is to monitor methodologies, suitably adjusted to the requirements and characteristics of the Norwegian society. Finally, our long-term study aims to investigate the security awareness of Norwegian internet users, with respect to various indicators such as age, gender, residence, educational background and work environment. 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 in the results. 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 a summary of the results from a study (Gunleifsen, 2019) sponsored by NTNU and Eidsiva bredbånd AS (Eidsiva bredbånd website, 2019) . In addition, we seek ways to create a training program for Norwegian internet users. Our results outline the generic properties of the population sample, and categorical differences within the delimited focus areas.

The remaining part of the paper is structured as follows: Section 2 explores the related work and discusses their limitations. Section 3 describes the research method. Section 4 presents results of the study. Finally, Section 5 concludes this paper and states the future work.

2 Related Work

Organisational studies (Kruger et al., 2010), (Hagen et al., 2008) have shown that collective employment participation and education are important factors in order to increase general security awareness. However, the NorSIS (Norsis, 2019) report from 2018 (Malmedal et al.,2018) states that cybersecurity awareness is not only an organisational culture, but it is a national and even a global culture. The Global

Information Technology Report from 2016 (Baller et al.2016), published by the World Economic Forum, shows that Norway is among the top 10 countries with the highest degree of digital service usage and digital readiness in respect of capitalising on digital platforms. Hence, studies of cybersecurity cultures in Norway are highly relevant due to their digital evolution. However, the NorSIS report has also shown how the Norwegian cybersecurity culture has not evolved for the last years and pinpoint that relevant education is national responsibility for Internet Service Providers (ISP), companies and the government. Together with Talib (Talib et al., 2010), they point out that cybersecurity cannot be achieved by technical means alone. Their studies have shown that the majority of cybersecurity training is undertaken both at home and at work.

Furthermore, from a threat perspective, people tend to alter their behaviour based on the amount of risk they perceive (Tariq et al., 2014). End-users that believe they are under a high threat, alter their behaviour to counter the consequences. However, when end-users of ICT systems believe they are not at risk, they become less cautious. Those 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 (Workman et al., 2008). This complicates the security awareness and results in a paradoxical situation where technical security solutions can degrade the security awareness of end-users (West, 2008). This is also reflected in business organisations 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 (Gkioulos et al.2017). The studies (Ariu et al.2014), (Gkioulos et al.2017), (Workman et al., 2008) show that the security awareness, in general, is low. Also, the general cybersecurity education is needed for end-users, including both for digital natives (Gkioulos et al.2017) and the older generations. However, these 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 concerns and a wide range of service providers. NorSIS discovered that security is not primarily taught from security specialists in organisations or generally in school, but end-users tend to learn from each other. 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 ISPs such as Eidsiva bredbånd. This study has looked into a new set of demographic attributes including i.e. Internet subscription owners, area of living and working sector, that is a combination we have not found in other studies (see Section 3).

3 Methodology

The data collection aimed to explore the security awareness of the residents in the rural areas of Norway. The target population resides in rural areas, primarily Hedmark

(194,000 citizens), Oppland (187,000), and parts of Akershus (575,000) counties. The target group was reached using the customer lists of subscription owners from the biggest ISP in the region, Eidsiva bredbånd. 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 to end-users. Eidsiva bredbånd primarily supplies to customers located in rural Norway, where 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 to approximately 10,000 customers and was live for 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 following areas of security awareness: Attitude, Knowledge, Risk evaluation, Trust, Training and Behavioural patterns. As for the level of measurement, the questionnaire had category, ordinal, and continuous type of 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.

To process the results of the questionnaire, we applied a variety of statistical data analysis methods available through IBM SPSS software v2.0. 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 evaluated 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. For these questions, we have analysed the median together with range, minimum and maximum values, and variance. Crosstabulation was applied to analyse the association between two category type questions, such as "Gender" and "Age." We have used Pearson two-tailed Correlation test to reveal relationships between pairs of variables as this test does not assume normality in the collected sample.

4 The results of the study

This section analyses and discusses the results of the survey. Firstly, we present the demographics in Section 4.1, followed by four sections of security awareness analysis where their general attitude towards cybersecurity (Section 4.2), their knowledge (Section 4.3), their risk evaluations (Section 4.4) and their trust (Section 4.5) in service providers and authorities are discussed. Section 4.6 analyses the training preferences among the users, while Section 4.7 compare their self-evaluated skills in knowledge and risk-evaluations with their actions and behaviour online.

4.1 Demographics

We surveyed gender, age, living area, education, employment sector, and the number of employees in their companies (not including Eidsiva bredbånd employees). 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 and gender skewness corresponds to their general base of customers. Their average age was relatively high, where 59% of the users were above the age of 56 years. The average age of all customers of Eidsiva bredbånd is 53.7 years and that they have 63,000 customers. The main reason for the average age is that the subscription owner is often a parent or a person that belongs to the oldest generation in a household. This age is not representative for the general population, but is a good representation of subscription owners although having a slightly higher average age. 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 inhabitants (Norwegian population website, 2019) with 6 largest cities have populations between 10,000 and 30,000. We let the users define if they were living in a rural area (25.9%), a village (28.8%) or a city (45.3%), 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 in the countryside/rural areas versus the people in the city.

Moreover, 64.0% of the respondents had a higher education, that is much more than the average population (33.4%) in Norway (Nowegian education level website, 2019). The last two demographic attributes we defined were the employment sector and the number of employees in their workplace (see Figure 1).

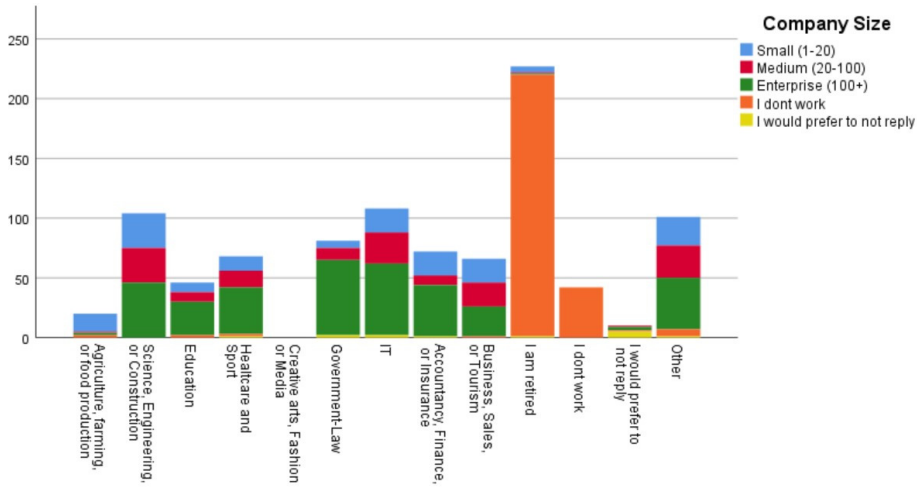

Figure 1: Distribution of employment sector and size

4.2 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, our assumption is that there is a high probability of reciewing a generally negative response or they 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.

As mentioned before, 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 cybersecurity. 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.

4.3 Cybersecurity knowledge

NorSIS report (Malmedal et al.,2018) stated: "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 the 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 any groups within the region differentiate themselves.

When evaluating the general level of knowledge, we noticed that there is a difference among the users in the self-evaluated level of knowledge. According to our findings (with respect to the number of female responses), we observed that men have a higher perception of knowledge. 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 is

therefore a relative scale that has been used by us and others (e.g. NorSiS). Our findings show that self-evaluation of knowledge is highly subjective and that it is a questionable parameter to use when measuring knowledge. The NorSIS report states that the level of knowledge about cybersecurity in Norway is good, but that it has not changed during the last years. A question such as "Do you know what cybersecurity is?", is a good baseline, but is highly subjective. About 90% of the users claim to be aware of online threats, while 77.8% claims to know what cybersecurity is, and 65% of the users were aware of any ICT regulation. This indicates that most users have a feeling of what cybersecurity is, but that their actual skills are highly subjective and also may not be as good as they think.

The subscription owners of Eidsiva bredbånd rate themselves as highly knowledgeable. If the actual level of knowledge is, in fact, higher for subscription owner of Eidsiva bredbånd, 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 cybersecurity than the rest of the population. The next sections measure how the level of knowledge correlates with trust and risk-evaluations.

4.4 Cybersecurity risk evaluation

Security awareness is closely connected to the perception of risk and trust. Evidence from other studies has shown that our willingness to take risks is closely connected to the level of knowledge (Parsons et al., 2010). The more we know, the more risk we are willing to take 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 cybersecurity incidents. However, we also know that we learn from the mistakes and from the incidents we are involved in (Malmedal et al.,2018). 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.

In general, the subscription owners of Eidsiva bredbånd are less worried and they are feeling safer than the national population. 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. 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.

Moreover, we discovered that increased confidence in skills makes us take bigger risks, which we particularly noticed for the age group of 36-55 years and for the users working with ICT (Gunleifsen, 2019). This pattern was especially seen for WiFi security. We also discovered that people below 35 years have a lower security awareness regarding phishing.

4.5 Trust in authorities and user responsibility

The NorSIS report (Malmedal et al.,2018) points out the importance of regulations and authorities in creating trust ICT ecosystem. This also includes that the society must accept and understand their responsibilities, their duties and their personal rights under these regulations. We measured 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 cybersecurity responsibilities.

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 tend to keep a higher personal privacy policy. This may have a connection to the fact that people who are working have a high interest in ICT and a high level of IT/security knowledge (Gunleifsen, 2019). Also, people have a high trust to authorities and they do know more about security laws and regulations than others.

Moreover, we observed from our findings that if the users have a higher security awareness, they put more security responsibility on themselves. Another observation is the importance of knowledge in order to be more aware of the cybersecurity threats, that indicates the general need for more training.

4.6 Education and training

It is identified that the self-evaluated level of knowledge is higher among the sample of subscription owners from Eidsiva bredbånd 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 regional differences cause this or if it is an attribute to subscription owners in general. However, it is expected that training in cybersecurity 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 of how this sample has trained and if they would start or continue training. This section also aims to identify how trained the respondents are, their training interest, how they would like to train and their stance towards training in cybersecurity. Moreover, we aimed to identify if there are any groups that would respond positively to customised cybersecurity training. Such questions about if and how the users want to train in cybersecurity are not covered in the NorSIS report.

We have identified that the sample of subscription owners of Eidsiva bredbånd are very positive towards cybersecurity training. However, the user sample (Gunleifsen, 2019) has in fact received much less cybersecurity training than the rest of the Norwegian population (Malmedal et al.,2018). Hence, the high level of self-evaluated knowledge is not explained by cybersecurity training.

We have noticed that people working in big companies have received more training than people in small companies. Also, we have noticed 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 informative 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 cybersecurity training than the people that work.

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

4.7 Cybersecurity behavioural patterns

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 consider a specific service or general case. The older generations are normally 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: about the unknown and about a certain threat. One example of this, we also found when analysing 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.

Another interesting observation is that we found three groups that are less concerned about their WiFi privacy than others: age group of 36-55 years, people working with ICT and people working with agriculture. These 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 found that the users consider it more secure to create a separate web-account with a separate user-names and passwords instead of using a centralised authentication service such as OpenID (Recordon et al., 2006). However, we also found 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, highlighting that larger companies have the resources to educate their employees and instil best practice policies in their professional life, which are then conveyed to personal praxis.

Regarding phishing, there seems to be a general awareness of the risk, 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 skills are willing to give away such personal information, witness that they have trust in their own knowledge and evaluation skills. It also might indicate that

they do not believe that the assets they have can be targeted by such attacks. Hence, this also indicates that they are willing to take bigger risks.

5 Conclusion and Future Work

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. We have also found that general cybersecurity awareness relies highly on individual perceptions, and that training, consequently, must be customised for the different groups.

We have also found that the level of knowledge affects the users' general stance towards privacy. A high level of knowledge makes 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.

The hypothesis that people working in big companies have more security training and therefore are more security aware, was supported. This indicates that this group of people does not need that much training focus from an Internet Service Provider perspective. Analysing the behavioural patterns within cybersecurity, 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.

We also raise the question if there is a security parallel between driving cars and cybersecurity. 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 fewer cybersecurity incidents than the rest of the population? For future work and upcoming surveys, it is recommended that the questions must be more nuanced in order to disclose this.

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.

6 Acknowledgement

This work has been supported by the Norwegian Internet Service Provider Eidsiva bredbånd AS and the CREATE project, of the Department of Information Security and Communication Technology, Norwegian University of Science and Technology.

7 References

Ariu, D., Bosco, F., Ferraris, V., Perri, P., Spolti, G., Stirparo, P., Vaciago, G., and Zanero, S. (2014). Security of the digital natives. Available at SSRN 2442037.

Baller, S., Dutta, S., and Lanvin, B. (2016). The Global Information Technology Report 2016. Technical report, World Economic Forum.

Eidsiva bredbånd website (2019), A Norwegian ISP. http://www.eidsiva.net (Accessed 22 May 2019)

Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., and Kotzanikolaou, P. (2017). Security awareness of the digital natives. Information, 8(2):42.

Gunleifsen, H. (2019). Cybersecurity Awareness and Culture in Rural Norway. Technical report, NTNU Open - Norwegian University of Science and Technology. Available online: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2592269/Norway_Security_awareness_gunleifsen.pdf (Accessed: 22 May 2019)

Kruger, H., Drevin, L., and Steyn, T. (2010). A vocabulary test to assess information security awareness. Information Management & Computer Security, 18(5):316-327.

Malmedal, B. and Røislien, H. E. (2018). The Norwegian Cyber Security Culture. Technical report, NORSIS - Norwegian Center for Information Security.

Merete Hagen, J., Albrechtsen, E., and Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16(4):377–397.

Norsis - Norwegian Center for Cybersecurity website (2019), https://norsis.no/ (Accessed 22 May 2019)

Norwegian educational level website (2019), https://www.ssb.no/utdanning/statistikker/utniv (Accessed 22 May 2019)

Norwegian population website (2019), https://www.ssb.no/kommunefakta/kostra/oppland/befolkningsprofil (Accessed 22 May 2019)

Parsons, K., McCormac, A., Butavicius, M., and Ferguson, L. (2010). Human factors and information security: individual, culture and security environment. Technical report, Defence Science Technology, Edinburgh.

Peters, G., Shevchenko, P. V., and Cohen, R. (2018). Understanding Cyber-Risk and Cyber-Insurance. Centre for financial risk, Macquarie University

Recordon, D. and Reed, D. (2006). 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.

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

Tariq M., Brynielsson, J. and Artman, H. (2014). The security awareness paradox: A case study. In 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014), pages 704–711.

West, R. (2008). The psychology of security. Communications of the ACM, 51(4):34–40.

Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in human behavior, 24(6):2799–2816.