NorSIS
Norsk senter for
informasjonssikring

THE NORWEGIAN
CYBER SECURITY CULTURE

Bjarte Malmedal & Hanne Eggen Røislien

Responsible: Roger Johnsen
Writers: Bjarte Malmedal
and Hanne Eggen Røislien
Layout: Maria Nyheim
Photos: Maria Nyheim

THE NORWEGIAN CYBER SECURITY CULTURE

Bjarte Malmedal & Hanne Eggen Røislien

INNHOLD

The ceo's perspective

It is a well-known fact that all Norwegians are online. Through this study we have found that Norwegians are confident that they are able to identify cyber-threats. Still more than half the population is worried falling victim to online fraud and computer viruses. They willingly accept state monitoring, but do not trust that the Police can help them if they fall victim to cyber-crime. On the other hand, almost half the population support vigilante and private law enforcement online. What does this tell us about Norwegian Cyber Security Culture and the prospects of successful digitization of public services and private businesses?

Human factors have long time been recognized as fundamental to cyber security. But so far efforts to understand this important phenomenon has been limited in scope. NorSIS sees mapping cyber security culture as a way of understanding yourself, your company and your country.

This project has been conducted to provide new insight in Norwegian Cyber security culture. Our goal is to develop effective cyber security practices and improve national cyber resilience. The results will also give indications on what security regulations the Norwegian people will see as acceptable and how to implement them.

Organized cyber-crime and foreign intelligence have long time analysed our cultural characteristics to disclose vulnerabilities to exploit. This gives them

definite advantages. Therefore, we should feel obliged to increase our understanding of the dynamics in how a cyber security culture is shaped and how it affects the digitalization in businesses, sectors and on a national level.

96% of all Norwegian are online, more than 90% embrace new technology, and 6 of 10 feel capable of judging what is safe to do online. Still cyber-crime costs Norway approximately 19 billion NKR annually. At the same time 73.9% argue that the Internet will not be safer even if their personal computer is secure. We have also found that a majority of Norwegians accepts that their online activities may be monitored by the authorities. But less than half the population believe the Police is capable of helping them if they are subject to cybercrime, and 4 of 10 sees cyber activists (e.g. Anonymous) play a role in the fight against cybercrime and cyberwar. 44% of the participants in this study say that they have refrained from using an online service after they have learned about threats or security incidents. This should obviously influence digitalization policy.

We argue that it is fundamental for a digitized society to enable its citizens to make good risk judgements. The educational system of today do not prepare us for the complex digital risk environment we all are supposed to engage in. In order to create a resilient digital Norway, it is paramount that the Government apply a holistic approach. The study at hand shows that it will be necessary to increase the reach and quality of cyber education, establish effective online law enforcement, and engage private and voluntary sector in a struggle to increase the national “cyber hygiene”.

Roger Johnsen
Administrerende direktør/CEO
Norsk senter for informasjonssikring

DNB

The need for a cyber security metric

Our society is undergoing a fast-moving digitalization in both private and public sector. Manufacturing, products and services are digitized, causing our national economic growth to be strongly linked to the digitalization efforts. According to The World Economic Forum in their Global Information Technology Report (2013)[1], we find that nations that already are highly digitized will experience a great effect in a further digitalization of their societies. A mere 10% increase in the digitalization can result in a 0.75% increase in GDP per capita. According to the report, Norway is the 5th most digitized country in the world, and thus has the potential to gain 24MNOK[2] per year as a result of a 10% increase in the digitalization . At the same time, cybercrime costs the Norwegian society large sums every year. According to the study on unreported cybercrime,[3] this amounts to 0.64% of the GDP per capita. This represents a potential loss of 19MNOK per year.

This paints a troubling picture. The digitalization has the potential to create economic growth and welfare through national and global trade, and more efficient public services. However, this potential is nearly eliminated as a result of an increased level of cybercrime. When adding the fact that foreign powers are stealing Norwegian technology research and development, the very thing our future generation will base their economy on, we understand that we need to do more to safeguard and protect our national ability to freely utilize the tremendous power that lies in the digitalization.

[1] http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf

[2] Estimate 2014

[3] *"Mørketalls-undersøkelsen"*, The Norwegian Business and Industry Security Council (NSR)

The efforts to safeguard and protect the digitalization are many, intertwined and complex. Our National strategy on information security (2012),[4] the Action plan for information security in the public sector (2015),[5] National security advice (2015)[6] and all the good work that is being put into this in the private and public sector all contribute to a digital robustness in our society. However, we know that we can't create a safe digital environment by technical means alone. Each and every citizen, employee and student must deal with a society that is driven by a rapid technological evolution and with a threat landscape that is constantly changing. How each of us perceive digital risks, and our attitudes and knowledge on how to protect our digital environment will in turn affect how the digitalization is happening. In a worst case scenario, this could lead to an unwanted development of the society where we as a nation is less willing to embrace the possibilities that the technology represents. A population that fears e-commerce will avoid it.[7] If we don't trust that the public sector can protect our personal information, we will resist governmental digitalization efforts. We are being bombarded with stories of everything that has, can and will go wrong, but are we really equipped to understand the actual risks at any given time or associated with any activity? We are concerned that we as a nation may get this wrong. That we, out of fear, overcompensate with security measures and that this will create a cooling effect on the digitalization, or that we choose inexpedient measures because we simply don't understand the risks involved.

Hence, we need to know more about cyber security culture on a national level and in our businesses. We need to develop a method for measuring cyber security culture. This will lead to a better and more efficient protection of our digital environment.

By using this method in both the private and public sector, we can obtain new knowledge that in turn will be a foundation for our national ICT governing politics and a way to assess the effects of security measures.

The Norwegian government is continuously developing its strategy on cyber security, and it released a revised action plan in September 2015. One of the strategic goals is to strengthen the cyber security knowledge and culture in the governmental sector. Whether you

[4] Ministry of Justice and Public Security

[5] Ministry of Local Government and Modernisation

[6] The Norwegian National Security Authority (NSM)

[7] https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

think that the human is the first or the last line of defence, it is beyond doubt that the human factor plays a key role in cyber security. In line with this, the Norwegian Centre for Information Security (NorSIS) is leading a project that aims to create a national metric for cyber security culture, which in turn will provide more a solid comprehension of how the Norwegian population relates to the inevitable digitalization of their society. The time for creating a national cyber security culture metric is long overdue.

For a nation, a deeper understanding about a cyber security culture is of utmost importance as it touches upon some of the most profound questions for development. Not only does digitalization help businesses make smart use of information technology and data, it ensures citizens benefit from the digital age and it underpins economic growth. A safe e-citizen is fundamental to the success of the national digitalization. Mistrust in digital services and fear of online crime are some of the challenges that people face in the digitalization processes. Thus, we must understand the dynamics in how a cyber security culture is shaped and how it affects the digitalization in businesses, sectors and on a national level.

Measuring cyber security culture

Creating a metric is a challenging task. In this section, we examine the difficulties in measuring culture and present an approach to creating a national cyber security culture metric.

The challenges of measuring culture

The main challenge in measuring cyber security culture is the concept itself. The emergence of the concept, as well as the day-to-day application of it, has made it problematic to utilize both vertically, amongst different types of business sectors, as well as horizontally, i.e. between different layers of society. The reason is simple: "Cyber security culture" is a concept first and foremost developed and applied within a business sector that is spearheaded by cyber security professionals and thus have cyber security as a primary focus. Thus, cyber security culture is a concept that has emerged within a rather limited and specialised cluster of industries, an industry with a sophisticated knowledge of cyber security paralleled by a keen interest in pushing the industry further. To put it simple: "Cyber security culture" is a concept developed amongst businesses that know what cyber security is. This does not hold true for a series of other types of industries, let alone for the Norwegian nation.

In creating a metric for measuring the national cyber security culture, there are at least two critical challenges: One is the question of terminology, i.e. what do we actually mean when we refer to "cyber security culture”? The other is the of level of analysis, i.e. how can we identify a “cyber security culture” concept that is valid and applicable to both businesses and nations? That is to say that whilst the concept might be developed within the confines of industries and businesses focused on cyber security, also nations have “cyber security cultures”. It may, however, not play out the same way. There is a huge gap in how “culture” is shaped and expressed depending on the level on which it is discussed. For example, whereas a business, an organisation and an institution all have defined purposes and thereby measures, the scope of a nation is much vaguer. Furthermore, while business can actively tutor and educate their personnel in cyber security, citizens of a state cannot be equally monitored. Is it, then, possible to generate a general comprehension of “cyber security culture” that is equally applicable to business and nations?

The term cyber security culture is not a new one, and there is no shortage in efforts to measure it. Although there doesn’t seem to be a clear and common understanding of the term, it is used to describe “something related to behaviour”. In other words: Cyber security culture is generally associated with the actions of employees. These are simple things to measure, so that is what the majority of cyber security culture metrics are set up to do. Different people grabs onto different aspects of cyber security behaviour. They measure and extrapolate their findings.

But; Does this really say much about a national cyber security culture? Is the percentage of the employees that click on a phishing-link a useful indicator of cyber security awareness, or could it be just as much about the skill of the attacker? More importantly, these studies fail to explain how awareness is developed, how our personal values shape what we think about cyber security specifically and technology in general, or what role our interests plays in how we relate to cyber security.

Cyber security culture as a tool

Cyber security culture is a concept increasingly acquiring awareness. Be it cyber professionals or businesses and industries specializing in cyber security; all agree on the fact that the numerous technical advances in information sciences do not always produce more secure environments. Human factors influence how individuals interact with cyber security technology and it is this interaction that is often detrimental to security. Therefore, it is evident that solely technical solutions are unlikely to prevent security breaches.

Organisations have realised long ago that the internal culture has critical impact on performance. It is the culture of the organization which extracts the best out of each person. The culture develops a habit in the individuals which makes them successful in the workplace. Yet, given the degree to which businesses have acknowledge the impact of culture to its performance, it is interesting to notice how immature the discussions on cyber security culture is. The fact that cyber security actually has a cultural dimension should not come as a surprise to anyone. However, judging from the discussions on cyber security culture, one could easily think that it is. Cyber security culture is overall approached in two, yet intertwined ways: Firstly, cyber security culture is considered as a tool in performance management. Secondly, cyber security culture is viewed as a sum of actions, a way the staff behaves. Generally, then, cyber security culture appears to be treated as behavioural patterns that can be altered and improved in order to increase the value added to a business or organisation. An obvious token of this approach is that cyber security culture tends to be discussed in terms of it being either “good” or “bad”. This normative overtone clearly indicates how culture in the cyber security context is seen as an aspect of utility, indicating that cyber security culture can be tested, measured and improved. This approach does, however, leave us with the obvious question: Is culture reducible to actions? And, is cyber security culture merely a tool for performance management and business governance? If so, it is tempting to ask whether the term “culture” may be imprecise.

In no other context can culture
be reduced to merely a set of actions.

In the social and cultural sciences, the term “culture” is considered far more complex and is rarely approached or described normatively. Rather, cultures are approached by scholars through a focus of the underlying ideas, values and attitudes that shape actions. Cultures are not tools; they place us in the world and shape our views. In other words, actions and behavioural patterns are the expressions of attitudes and values.

Towards a holistic approach to cyber security culture

There appears to be a clash of scholarly disciplines in the comprehension of “cyber security culture”. This does not come out of the blue: cyber security and cultural studies have thus far been rather separated scholarly disciplines. The scientists dealing with culture have very rarely dealt with cyber security – and technologically schooled professionals have left culture to be studied by others. The reason is obvious: If you are an expert in cultural or social sciences, you do not have the skills to comprehend – or even engage in – the specialised language of engineers and cyber professionals. Yet, we believe that the analysis of cyber security culture benefits from a more comprehensive approach, wherein the competencies of cyber-professionals and cultural scientists are integrated.

We believe that measurements of cyber security cultures can benefit from a more comprehensive approach, taking a step back from simple registrations of whether employees open phishing-emails and rather look at the attitudes and perspectives towards technology and cyber security, and how this resonates with other core values, interests and abilities.

syljuåsen

Method

Cyber security culture is a complex matter and that the mechanism that influence it are, to a large degree, unknown. The lack of knowledge in this field presents us with uncertainties regarding what the indicators for cyber security culture really are. Does age play a significant role? Or should we look into the size of the company? Or perhaps the type of company, and the cyber security training its employees are given are more significant? What if new knowledge can be found in the combination of such factors?

This may present us with some challenges regarding the validity of the indicators. We approach the uncertainty regarding the validity of the indicators in several ways: We include a wide variety of indicators in order to explore them further in the analytic work, we conducted a comprehensive pilot study in 2015 where the indicators were tested and validated. Finally, we utilize the network of cyber security professionals in the project reference group to ensure the quality and validity of the indicators.

The study is targeting the Norwegian population, and we made an extra effort to create indicators that are meaningful for people of a broad age range, of different education levels etc. The reliability of the indicators is dependent on the fact that everyone will understand the questions in the same way, and that the meaning embedded into their answers are the same. We believe that the indicators are robust, and that they can be used across sectors and businesses. We also believe that the indicators are robust over time and that this will enable us to follow the same group over years, and learn how the cyber security culture changes or evolves over time.

A robust and standardized set of indicators will enable us to create a baseline for the national cyber security culture, and to do meaningful comparisons between sectors, businesses and groups in the population.

Data collection is ensured by sending an electronic questionnaire to a large number of recipients. We approached 29 Norwegian companies and organizations, based on a set of selection criteria such as the type of sector/industry they belong to and the estimated demographic profile of their employees, students, customers or members. In addition to this, the indicators were used in an omnibus to ensure a representative baseline.

Research questions

Our study focus on how the national cyber security culture relates to, and possible influences, the digitalization in the public and private sector. In this context, we formulate these research questions:

- What characterizes the Norwegian cyber security culture?
- To what degree does cyber security education influence the Norwegian populations cybersecurity behaviour or awareness?
- How does the Norwegian population relate and react to cyber risks?
- To what degree does the individual take responsibility for the safety and security of the cyberspace?

In order to answer the research questions, we structure this report into the following chapters:

The Norwegian cyber security culture

Competence, knowledge and learning

Risk perception

Behavioural patterns

Indicators of cyber security culture

Based on the research questions, we have developed a set of indicators, questions, that may provide data suitable for answering the research questions. The indicators are put together as an electronic questionnaire in both Norwegian and English. There is a slight difference between the two: Some of the background variables are adapted to better suit participants outside of Norway.

The Norwegian questionnaire is presented in Appendix A. The English questionnaire is presented in Appendix B

The demographics

The total number of respondents in this study is 8193. The 6000 respondents from the pilot study are left out because the questionnaire used in the pilot is slightly different from the one used in the study. The study also included a number of surveys from 12 other countries as well as English-speaking persons in Norway. However, those respondents are also left out of this study because the numbers are too low to provide statistically significant results.

SEX	#	%
Female	4252	51.9
Male	3941	48.1
n=	**8193**	

AGE	#	%
Under 15	144	1.8
15–19	628	7.7
20–25	164	2.0
26–35	940	11.5
36–45	1576	19.2
46–55	1855	22.6
56–65	1553	19.0
66 and over	1333	16.3
n=	**8193**	

EMPLOYMENT IN SECTOR	#	%
Private sector	2213	27.0
Public sector	3978	48.6
Unemployed	2002	24.4
n=	**8193**	

HIGHEST EDUCATION LEVEL	#	%
Primary school	580	7.1
High school	1779	21.7
College (Bachelor's degree or similar)	2749	33.6
University (Master's degree or above)	2610	31.9
Other	344	4.2
I choose not to answer	131	1.6
n=	**8193**	

Table 1: Demographics

COUNTY OF RESIDENCE	#	%
Akershus	1214	14.8
Aust-Agder	89	1.1
Buskerud	576	7.0
Finnmark	47	0.6
Hedmark	148	1.8
Hordaland	810	9.9
Møre og Romsdal	157	1.9
Nord-Trøndelag	105	1.3
Nordland	175	2.1
Oppland	537	6.6
Oslo	1538	18.8
Rogaland	578	7.1
Sogn og Fjordane	90	1.1
Sør-Trøndelag	366	4.5
Telemark	128	1.6
Troms	149	1.8
Vest-Agder	107	1.3
Vestfold	291	3.6
Østfold	1088	13.3
n=	**8193**	

As we see from these numbers, the dataset contains a low representation in the age group 20–25 as we were unable to form a partnership that would enable us to reach this group in particular. The dataset does however contain a satisfactory representation in the age groups below 20 and above 66, as well as the group that is unemployed. Normally, cyber security culture studies are conducted within businesses, and does not include data for these groups.

The percentage of the unemployed is higher in our dataset than the official numbers by the Statistics Norway.[8] This is explained by the overrepresentation of students in the study.

Cyber Security vs. information security

The terms cyber security and information security are often used as synonyms, although they are not.[9] [10] [11] Information security refers to the protection of all information, in which some of it can be digital. Cyber security refers to the protection of everything that is vulnerable by means of ICT. For our purposes, cyber security seems to be the term that is best fit of the two. This study does not concern itself with information that is not digital. We still believe you shouldn't throw away information on paper that "dumpster-divers" can find and use to commit ID-fraud, but we are concerned with so much more than just the information itself. Hence, information security is a term that is too narrow for our purposes, and it can be misleading since we are not concerned with analog information.

[8] https://www.ssb.no/arbeid-og-lonn/statistikker/regledig

[9] von Solms R, van Niekerk J, "*From Information Security to Cyber Security*", Computers & Security (2013), doi: 10.1016/j.cose.2013.04.004

[10] http://www.govinfosecurity.com/blogs/cybersecurity-vs-information-security-p-711

[11] http://mortenirgens.com/?p=769

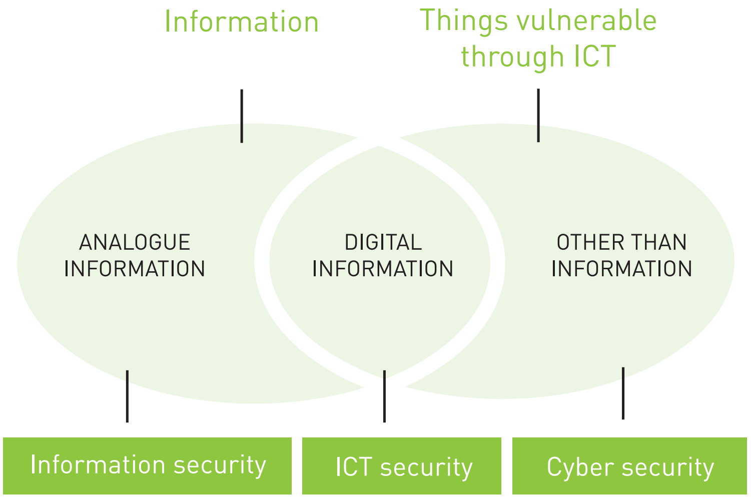


Figure 1: Cyber Security vs. Information Security

Cyber security can mean the protection of ourselves from online bullying, how we protect our civil rights from surveillance or how resilient we are from cybercrime. We acknowledge that some place a more technical understanding into the term cyber security. However, we believe that the “things” that are protected through cyber security reaches far beyond the technical realm.

DESIGN & CULT
EPLEMOST

The norwegian cyber security culture

Understanding cyber security culture: Key components

Among the features that differentiates nations, culture is one of the most dominant ones. All nations have cultures. National cultures shapes who we are as a group, and how we as individuals orient ourselves in the world. In other words: National cultures functions as glue amongst the citizens, and relates to our deeply held values regarding such as what we consider as normal versus abnormal, safe versus dangerous, and rational versus irrational. Our national cultures offer a set of values that help us make sense of our surroundings by establishing a compass that tells us "how we do things". The result is that national cultures comprise systems of shared values, preferences, and behaviours of population groups that differ widely between countries. These cultural values and norms are learned at an early stage in life, and is passed on both formally (at school, our workplace, in our leisure time activities etc.) and informally through interaction with friends, parents, siblings and others. As a result, national cultures are deeply rooted in us, and last over the course of generations.

Still, national cultures are not clear-cut and do not come in a "one size fits all" format. They are comprised of multiple sub-cultures, wherein factors such as age, geography, interests, focus-area and gender come into play. Cyber security is one such sub-culture. Today, it is safe to say that cyber security is relevant to nearly every one of us, given the degree to which our societies are increasingly digitized. In other words: All nations have cyber security cultures. We write on computers, have our eyes fixed on our smart-phones and buy our groceries and clothes online, while we pay our taxes through the government's website that we log on to with the chip and code we are given.

However, cyber security cultures have thus far been considered a part of organizational cultures, thereby a concern for businesses and industries. As a consequence, cyber security culture has been treated as a tool for organizational efficiency and success. Yet, organizational cultures differ from national cultures on the most fundamental level: Whilst national cultures concern the shared values and norms, organizational cultures are based on shared practices.

Organizational cultures are based on broad guidelines, which are rooted in the organizational practices that businesses not only teach their employees; organizational cultures are comprised of norms and practices that businesses expect their employees to follow. If they do not act according to them, they may lose their jobs.

This is of course not to say that organizations' cyber security cultures are less significant. However, they are something else than national cyber security cultures. Moreover, they are less deep-seated than cyber security cultures on a national level.

There are a number of definitions of cyber security culture, and whilst there is as of yet not one definition all cyber security professionals seem to be able to gather around, they all converge around the same key issues: All security is about the protection of assets from the various threats posed by certain inherent vulnerabilities, and cyber security is consequently about protecting the information assets. Cyber security culture, then, is the attitudes, assumptions, beliefs, values, and knowledge that people use in their interaction with the information assets. Thus, cyber security culture is comprised of behaviour and a set of ideas and attitudes.

Thus far, most studies of cyber security culture focus on the behavioural dimension. That is, they focus e.g. on the degree to which employees click on phishing links, or whether or not they share their passwords. As a consequence, although the general notion is that cyber security culture contains elements of values and attitudes, the way it is dealt with tend to set these elements aside in favour of a focus on behaviour.

As we see it, the focus on behaviour in the context of cyber security culture can say something about what people are doing or have done. However, it may say very little about what they will do. In other words, focusing on behaviour can project an image of security conduct in the past ("this is what they did"), but it can say relatively little about the future. Yet, we strive to increase security predictions. That is to say that timely security measures must be one step ahead. Thus, instead of being able to portray what people have done or how people have used to behave, one should rather be able to have a credible prediction of what people are most prone to do in certain situations. In our approach to cyber security culture, then, we have chosen to downplay behaviour and rather focus on attitudes, values and sentiments that can say something about what people will do, or how they will respond.

This focus has led us to ask the inevitable question: Which key traits characterize attitudes, values and sentiments in any given cyber security culture? What elements comprise the basis of a cyber security culture?

In our study, we have mapped the core traits of the national cyber security culture in Norway. We departed from the assumption that national cultures – and thereby also cyber security cultures – cannot be approached merely as behaviour: Rather, the national cyber security culture ought to be considered as a set of values, sentiments and attitudes regarding a given topic, i.e. cyber security. Cyber security on a national level relates to a wide set of themes, ranging from governance and state control to individual notions of technological competence and risk-taking.

Any culture balances between the individual and the collective, between individual judgements and perceptions and collective norms and standards. We are neither completely individual, nor are we completely part of the larger collective. Conceptualizing cyber security culture, then, implies pinpointing those factors that not only comprise cyber security culture as a whole, but that also highlight the central debates and challenges of cyber security culture that together constitute the building blocks.

With that in mind, we have singled out eight core issues that comprise cyber security culture as we see it. These are:

- Collectivism
- Governance and Control
- Trust
- Risk perception
- Techno-optimism and digitalization
- Competence
- Interest
- Behaviour

In the following we will present the main findings, based on our eight core topics. These results do say something about where the Norwegian citizenry situate themselves compare to the general population. However, the numbers will be given more depth when compared to similar figures from other nations.

Collectivism

Cultures are per definition collective. Cultures are comprised of individuals: Cultures are developed by individuals, whilst at the same time contribute to shaping the individuals that are part of any given culture. Cultures point to the characteristics of a particular group of people, including such as their social habits, their attitudes, their values and priorities. Cultures necessitate some degree of solidarity amongst the members. That is to say that in order to last, cultures necessitate loyalty and solidarity. The individuals must identify themselves as part of the group, contribute to it, and adhere to the explicit and implicit norms of behaviour. When singling out collectivism, we wish to point towards how the individual relates to the collective. In so doing, we point at two themes: Firstly, to what degree individuals see themselves – if at all – as part of a greater "cyber collective". And, secondly, whether individual behaviour as shaped by collective norms and behaviour.

Governance and Control

With reference to collectivism, governance is a collective term that refers to the questions of how the collective should be regulated and by whom. Hence, the issue of governance refers to the users' views on governance and control of information and communications technology (ICT). A critical issue here is e.g. the question of surveillance: Who are responsible for drawing the red lines of what is acceptable in the use of ICT, where should these lines be drawn and how should citizens abide to these lines?

By raising the issue of governance, then, we wish to draw attention to the question of who is responsible for our safety online. In the context of security, there is always the question of how to balance between individual freedom and collective safety. "Everybody" wants freedom and "everybody" wants at the same time to be safe. How does this balance play out in a given cyber security culture? How much surveillance is acceptable when individual safety is at stake?

Trust

Trust is a cornerstone to any viable democracy. Democracies depend on trust in a whole variety of forms: A well-functioning democracy necessitates trust amongst its citizens, amongst citizens and the government, between governmental institutions, between business, between citizens and their employer and so forth. In other words: Trust is a prerequisite for economic welfare, stability and growth in a country. As more and more of our national growth is tied to the digitalization of the nation, trust in this area is of great significance.

For authorities to govern efficiently and in accordance with the law, while at the same time maintaining stability, they need not only to have the jurisdiction on their side: They need trust from the citizens. This implies that authorities must be allowed to govern also when e.g. executing policies that citizens may disagree with, or when implementing measures that are alien or new to citizens.

As a consequence, the process of digitalization both relies on, as well as it is vulnerable to, trust. The process of digitalization is encouraged by the authorities in almost all nations, and given the development of technology in our era, the digitalization of our societies is inevitable. But, citizens are not only encouraged to apply increasingly more technological tools; they are forced to do so. For example, in Norway you are not able to oversee your taxes without logging into a website run by the government. Not paying your taxes results in huge fines that can be detrimental to individuals and companies. Thus, if you do not log on to the website, you cannot verify your taxes, which in consequence will cause you serious financial and other legal problems.

Yet, whilst demanding the public to employ digital tools may cause less paperwork and thereby benefit the bureaucracies, it assumes trust from the citizens. For one, public services must be secure. The public does not tolerate many security breaches before they not only avoid using the website or the service; they may also stop trusting the authorities.

The types of trust necessitated are obvious: Trading and shopping online is becoming increasingly common. When shopping online, we submit our credit card details and hand over other personal information. In so doing, we trust that the company treats the data with care. Yet, this is already a balancing act. It is come to the fore that Google, Apple as most of the other technological companies now use the information they gather in order to profile their users. Profiling, in turn, is used as a tool for marketing, for targeted advertising, and for companies to push their products. This allows us to ask: Must buying a book online through e.g. Amazon also imply that I necessarily open up for other companies to target me with their products?

Targeted advertising is the flipside of the coin in terms of digitalization and trust. Targeted advertising is to many a breach of trust, as it is a result of how websites have used the information we are forced to provide to their own gain. This leads to a lack of trust and potentially a threat to the process of digitalization.

Risk perception

Competence, learning and risk are tightly knit together. For example, studies have shown an increase in so-called "risky behaviour" amongst individuals who have a high level of competence or perceived skill. Hence, it is likely that people who have skill in the area of cyber security could overestimate their ability to control the threat, and they may therefore take more risks.[12]

In a study by Kathryn Parsons, Agata McCormac, Marcus Butavicius and Lael Ferguson in the Australian Defence Science and Technology Organisation, risk is highlighted as a key factor in the formation of behaviour. According to the study, individuals are found "to have an unrealistic optimism for risks that they perceive to be under their personal control".[13] [14] They argue that since "an individual may view their actions on their personal computer to be under their control, threats may be seen as less risky. Hence, the chance that non-adherence to security policies will result in serious consequences may also be underestimated. This means that individuals might be more likely to engage in risky behaviour".

Techno-optimism and digitalization

Not only does digitalization help businesses make smart use of information technology and data, it ensures citizens benefit from the digital age and it underpins economic growth. By focusing on techno-optimism and digitalization we want to transgress the mere fact that digitalization is part of how our societies develop. Instead, we want to draw attention to citizens' attitude towards this societal tendency. In other words: Your attitude towards digitalization influences how you relate to technology. A safe e-citizen is fundamental to the success of the national digitalization. Mistrust in digital services and fear of online crime are some of the challenges that people face in the digitalization processes. Thus, we must understand the dynamics in how a cyber security culture is shaped and how it affects the digitalization in businesses, sectors and on a national level.

[12]: Parsons, McCormac et al. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment*

[13]: Ibid.

[14]: Kreuter, M.W., & Strecher, V. (1995). *Changing inaccurate perceptions of health risk: Results from a randomised trial. Health Psychology*, 14, 55–63

Competence

As everything from social services and state tax payment to individual communication and the sharing of holiday photos are happening online, citizens are forced to make use of ICT, regardless of whether they appreciate it or nor. This implies that citizens must acquire a digital skill-set that makes them capable of being part of modern society. Consequently, all citizens of Norway must have fundamental digital skills. The question is: Where and how do they acquire this skill-set? The paradox today is that most countries push their citizens to go online, and our societies' development depend on a comprehensive process of digitalization. Yet, a thorough digital skill-set is rarely taught in schools. The general public must therefore acquire this skill-set through informal channels.

In all cultures, some people are listened to, to a larger degree than others. Be it celebrities, national pundits or experts – some are given the microphone more often than others and influence our opinions. National pundits and celebrities have crucial impact on cultures; who we admire and who we listen to shape our attitudes and our values, and thereby contribute to shaping how we relate to others and how we behave. Who are the significant voices in teaching us our cyber security skills? Do different people speak to different groups of society? What constitutes these differences?

Interest

In a society that is increasingly digitalized, one may be tempted to conclude that citizens with an interest in ICT have an advantage over those citizens that lack this interest. Interest shapes our attitudes, our skills and our knowledge. Interest influences who we relate to and thereby who we learn from. With interest comes awareness, curiosity and time. These are cornerstone in learning. It follows that one may wonder whether people with an interest in ICT learn faster than those who lack such an interest. Therefore, interest appears to be decisive in a digitalized society.

Behaviour

Most studies of cyber security culture focuses on behaviour. This is not without reason: after all what we do is not only the easiest thing to measure; it is also what we do that most concretely influence our cyber security and the digitalization of society.

In terms of cyber security there are certain types of behaviour that are encouraged, whilst others are warned against. Governments, authorities, business leaders and experts provide advice that form a normative standard for how citizens or employees should strive towards behaving. However, given the rapid development of technology, this “best practice” standard is perishable. That is to say, that expert advice and norms for ICT behaviour have changed over time. As a result, going through training and courses in information technology once does not suffice: It must be repeated. What you learned 10 years ago may not be merely “dated”; it may just as well be wrong.

When surveying cyber security cultural behaviour in 2016, there are still a number of things we encourage citizens to do: Citizens should not share their passwords with others; they should make security copies of their information and update their software regularly. Citizens are encouraged to do so in order to reduce the likelihood of hacking and computer crime, to prevent the loss of information, to reduce the possibility of manipulation of information and so forth.

Measuring the behavioural patterns of the Norwegian cyber security culture, then, implies two things: Firstly, we want to paint a general picture of the behaviour of Norwegians in the context of cyber security. Secondly, we want to see to what degree Norwegians comply with the “best practice” norms of behaviour communicated to them.

Our findings

In the following we describe the characteristics of the Norwegian cyber security culture.

Collectivism

It is challenging to assess the degree to which Norwegians associate themselves with a “cyber collective” or an “online cyber security culture”. One indicator could be the issue of anonymity, as limitation of the ability of being anonymous is reported to have a positive effect on challenges such as cyber bullying and harassment. Still, the majority of Norwegians, 59%, respond that they agree with the statement that “It should be possible to be anonymous on the Internet”.

Another indicator could be the degree to which their own computer and activity has impact on the collective. Yet, an overwhelming 73.9% argue that the Internet will not be safer even if their personal computer is secure. However, this statement may also reflect lack of competence of what cyber security is in practice.

Governance and Control

The majority of the population express a positive attitude towards governance and surveillance of their online activity. 59% respond that they are benign towards the fact that their online activities may be monitored, given that it contributes to making them safer online. Interestingly, we find that political ideology does not play a large role in this matter. With the exception of the people who associate themselves with the liberal political party, more are positive towards surveillance, given that it contributes to making them safer online.

The degree to which Norwegians trust the police or other law enforcing bodies to assist them if they are subject to cybercrime is, however, low: Less than half of the population (45.8%) agree with the statement that "Law enforcement agencies will help me if I am subject to cybercrime". 36.5% disagree to the statement. These finding correlate with the Norwegian Police's documentation of trust amongst the citizens in 2015, wherein approximately 75% of the population had a negative impression of the police's ability to assist them in cybercrime. Furthermore, we find that 41.1% agrees with the statement "Cyber activists (e.g. Anonymous) play a role in the fight against cybercrime and cyberwar". This may indicate that there is an erosion of the principles of who and how the exercise of power should be in the cyber domain. We still find that most people think that the police should protect them from criminal activities such as ID-theft and online fraud. 92.9% say that they would report ID-theft to the police, and 85.6% say they would report online fraud. These indicators should be watched closely so one can discern negative trends early and implement corrective measures.

Norwegians do seem to be concerned about their privacy: 38.1% disagree with the statement "I accept that my activities online ae monitored if it makes mesafer online", and 59% thinks that it should be possible to be anonymous online. An overwhelming 90.6% respond that they would make sure that all personal data would be deleted if they were to sell or throw away their personal computer.

Trust

One of the reasons why the Norwegian democracy functions so well, is the fact that Norwegians express trust towards their surroundings: They generally trust their neighbours, they trust their employer and they trust the government. That is to say that Norwegians do not expect to be robbed by their neighbours, that their employer won't pay their salary or that the government is corrupt without providing for the welfare of the state.

It is well-documented that the Norwegian society is characterized by a large degree of trust.

In line with this, it is perhaps not surprising that the respondents have reported that 65.4 % trust that they authorities will process and store the personal data they have provided in a secure manner. Accordingly, also 70.8% of the population report that they think they do not expose themselves towards a considerable risk when using online banking, whilst only 10% report that they consider online banking to include risk-taking. Also, 61% of the population feel safe when they use public services online, whilst only 12.6% of the respondents' report that making use of public services online also implies taking a risk.

Interestingly, 18.1% think that Norwegian web-sites are more secure, and only 0.2% think that foreign web-sites are more secure. 29% report that Norwegian and foreign websites are equally safe and another 39.6 % respond that what is decisive is whether the website is well-known or not.

Risk perception

Risk perception is highly subjective, but even so, it's a powerful factor that greatly influences how we think and act when it comes to digital threats. It is a factor that, to some degree, can't be calculated or predicted, although we know that it can and will be influenced by security events, what we think we know about digital threats, our experiences in the past etc. 72% of the participants in this study think that they expose themselves to risk when they use the internet, and nearly as many (70%) are of the opinion that they are receiving adequately information about the digital threat. Furthermore, we find that 61% of the participants think that they are able to assess what is safe to do online, while 23.5% think that they can't make such an assessment.

Over two thirds of the population, that is 67.8%, respond that the biggest risk online is that someone else will do something to them online, such as hack a website where they have provided personal data. This may reflect the Norwegians' general notion of their relative competence regarding cyber security. In other words: Norwegians' confide in their own ability, but express concerns about other people's intentions.

Risk perception and competence overlap in several instances. For example, to the question of whether knowledge about threats or hacking has led the respondents to refrain from using a service online, the answers are split in two: 44% respond that such knowledge has made them refrain from using an online service, whilst 42.5% respond that it hasn't. Thus, there must be other factors at play when people refrain from using an online service.

Norwegians are, in general, not very worried about risks associated with most online activities. Only 10% are worried about using online banking, and a mere 12% are worried about using public (government) services online. When we ask about their own security practices, they clearly show a competence in what is considered "best practice". 85% associate high risk with the practice of sharing their password with others, 61% associate high risk with the practice of using the same password at several online sites and 63% thinks the same about not back-up their data regularly.

Techno-optimism and digitalization

The Norwegian cyber security culture is overall characterized by a strong positive attitude towards technology. As much as 96.7% of the respondents answer that they are positive towards making use of new technology. This markedly positive attitude towards technology is paralleled by the fact that 89.9% of the respondents say that they know what cyber security is.

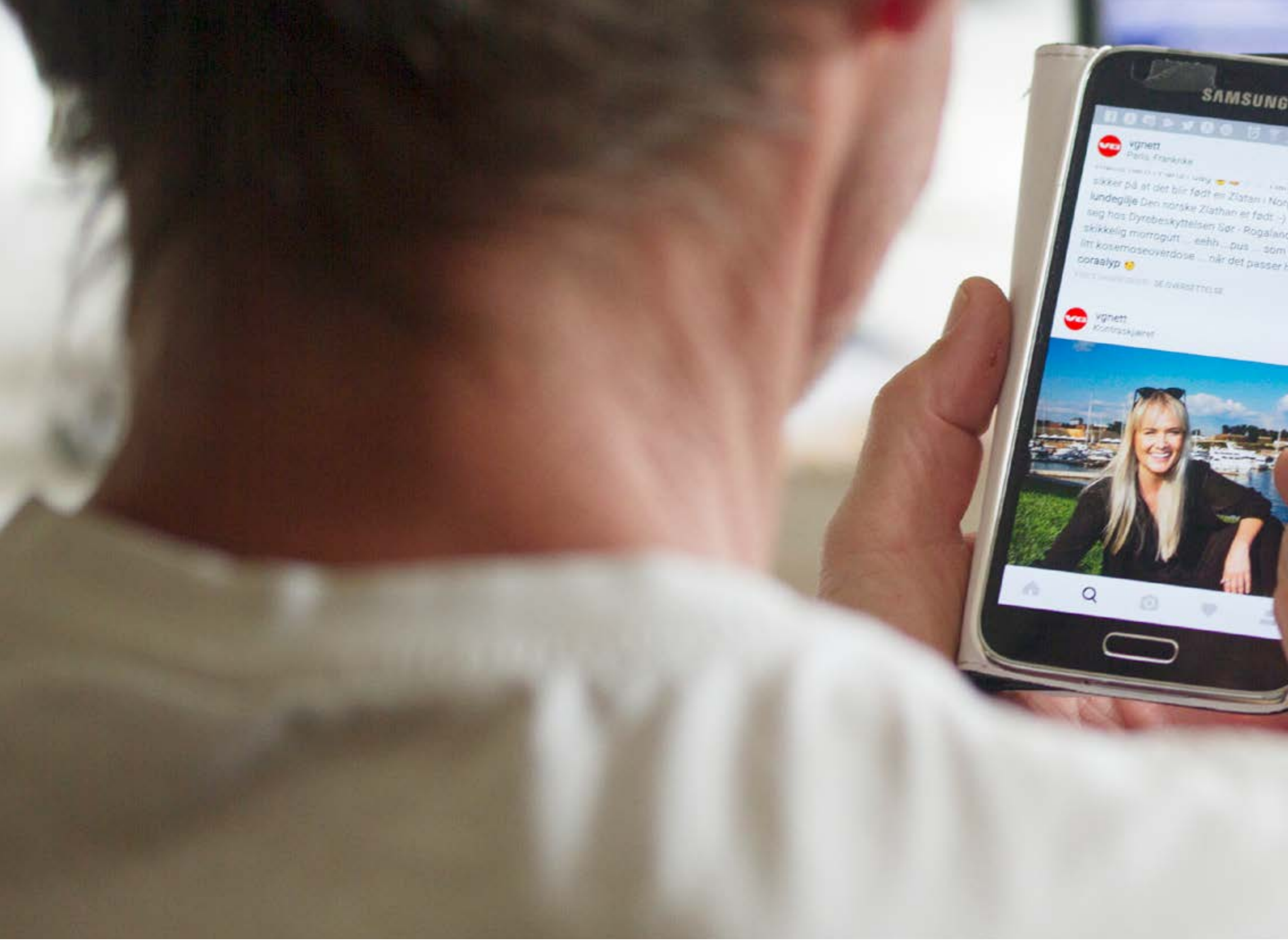
Competence

The Norwegian population is generally rather competent when it comes to cyber security. That is to say that they view themselves as rather knowledgeable and therein also consider themselves to be able to make important considerations and judgement calls in the area of cyber security. Norwegians generally consider themselves to know as much as the others or a little more. That is to say that 57.4% consider themselves to know "more or less the same as the average", whilst 33.4 % respond that they know more than the average population.

The majority of Norwegians claim to be able to make important considerations and assessments in the cyber security domain. As much as 61.1 % respond that they feel capable of judging what is safe, or unsafe, to do online. 15.3 % respond that they do now know the answer to that question, whilst nearly a quarter of the population (23.5%) feel unequipped to make such judgement calls. Another 70.1 % also report that they are of the opinion that they receive sufficient information about online threats.

Interest

Nearly half of the population (47.1%) report that they are explicitly interested in technology and IT, while an additional 33.6% respond that they are neutral towards technology. Only 18.6% respond that they have little interest in technology and IT. In sum, an overwhelming majority of the population thus have a benign interest in technology and IT, which is in line with overall positivity in making use of new types of technology.

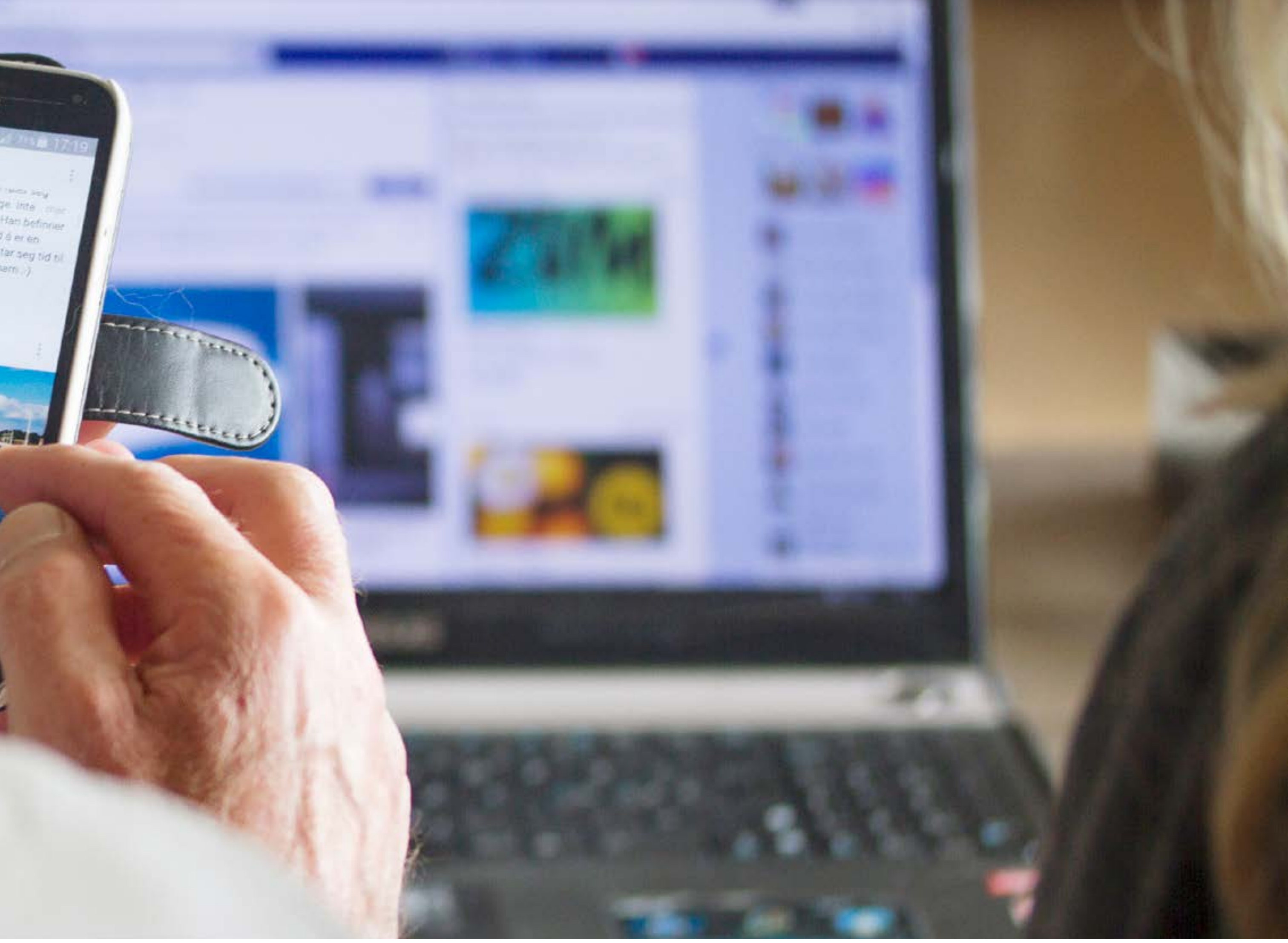


Behaviour

Three quarters of the population say that they assess whether a website is safe before using it, but only 7.8% say that they always do this. It should be noted that only 61.1% say that they know how to do do that kind of assessment.

While we encourage everyone to abide with what we consider to be safe password behaviour, we still find that 18.5% say that they use the same password everywhere. Password managers may enable us to use more complex passwords, but we find that only 9.2% say that they use these kind of tools. It's slightly more satisfying to observe that 61% say that they use different passwords for most online services, and that 37.8% say that they try to create secure passwords.

18.0% say that they have no routines for updating their software, and 6.6% say that they don't know whether they have such routines. This means that a rather large portion of computer systems are left vulnerable for cyber criminals to exploit.



14.7% say that they never back-up their information, and 9.3% say that they don't know whether they do or not. The majority (41.5%) back-up their data less than every month.

Security software may provide a defence against cyber criminals, and we find that only 2.6% say that they have no security software at all. 9.3% say that they don't know if they use such software. 61.3% say that they use some kind of firewall, and 73.8% say that they use anti-virus. We can assume that these high numbers can be explained by the fact that most vendors ship computer systems with security software pre-installed, and that it is not necessarily a choice on the user's behalf.

We find that 9.5% of the population say that they sometimes deliberately break cyber security regulations.

Competence, knowledge and learning

Introduction

The technological advances in the cyber security field are numerous, however the advancements in technology alone is not always enough to create a more secure environment. The use of strong encryption and more secure operating systems and programs makes it harder to exploit computer systems, thus forcing cyber criminals to adapt. There is a clear increase in internet related fraud, as well as other online crimes. This may indicate that cyber criminals are shifting their focus, from attacking our computers, to attacking us.

Our interactions with information technology, and the risks associated with them, are changing and becoming more complex.

As society becomes increasingly dependent on technology, each individual is given more responsibility. We expect everyone to understand the risks associated with our online activities. This means having current knowledge about a threat that is constantly changing as well as new technological advances and their inherent and interdependent vulnerabilities. We expect everyone to exhibit a safe and secure online behaviour, even if this too is subject to change. (Do you change your password every so often, and refrain from writing them down? Well, now we recommend that you DO write them down,[15] and that you don't change it unless you think it has been compromised[16]).

[15] https://nsm.stat.no/blogg/er-sommerferie-2014-et-bra-passord/

[16] https://www.cesg.gov.uk/articles/problems-forcing-regular-password-expiry

This places a tremendous responsibility on the individual. We expect everyone to understand and to behave according to both explicit and tacit knowledge and norms. Companies approaches this with cyber security education and awareness campaigns, but do little to assess the effectiveness of their efforts. People not under employment, or employed in companies that don't educate their workforce in cyber security, are more or less left with the public education system, to informal transfer of knowledge or to themselves.

There is a need for a deeper understanding of how competence and knowledge are formed. How do we learn about cyber security? Does cyber security education really have an effect on how behavioural patterns are formed?

Our findings

The study shows that 50% of the participants in this study has received cyber security training during the last two years, while 44.5% has not received such training. 5.4% does not know whether they had training or not.

HAVE YOU RECEIVED CYBER SECURITY EDUCATION DURING THE LAST TWO YEARS? (RESULTS IN %)

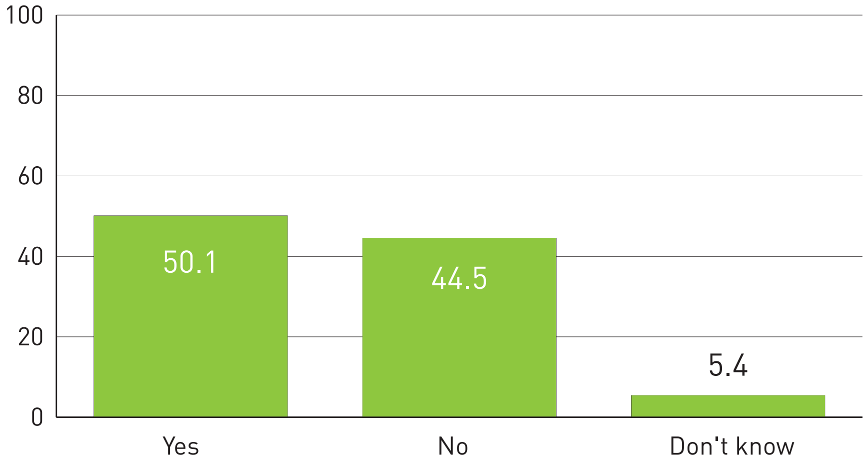


Figure 2: Cyber security education

When we break down these numbers, we find that for people in the age group below 20, a mere 28.4% receive cyber security education. We discover a similar finding for the age group 66 and above, where only 17.5% have received such training. Both findings show a significantly lower rate than for the average population. However, when looking at the group in employment, we find that 53.2% in the private sector, and 63% in the public sector has received cyber security education during the last two years. People who are currently unemployed report that only 21% have received such training

We are particularly interested in whether the cyber security education and training has an effect, and to what degree we can describe the effect. When asked, most people think that the cyber security education has improved their cyber security skills. 77% thinks this is the case, while 10% disagree that their skills have improved. Nearly 13% does not know whether it did or not. These numbers are consistent for all age-groups, for both private and public sector and for all company sizes.

Further, we have looked into certain aspects of self-cognition related to cyber security education and its effect on how people assess their cyber security skills. Of the people who have received cyber security education, and who think that it has improved their skills, 45% believe that they know more about cyber security than average. This is a clear increase from the population as a whole, where 33% place themselves above average. We notice a small increase in how people see their abilities to assess what is safe to do online, from 61% in the general population to 68% for the group that has received cyber security training.

On a national level, it is not the security of the individual computer that matters, but that enough of them are.

However, we find no correlation between cyber security education and the belief that the internet becomes more secure if your computer is secure. This may imply that the cyber security education that is provided makes little effort to properly explain the complexity of cybercrime, and how personal computer systems are used in criminal “value-chains”, for example that DDOS capabilities in fact are enabled mostly through unsecured computers. There is a notion in the field of cyber security that “cyber security hygiene” is a key component in the overall resilience against cyber threats. Comparable to vaccine programs, enough computers must be secured in order to effectively disrupt certain criminal value chains.

We have also looked into how people learn about cyber security, and who they learn from. In general, people learn from three different sources. Themselves, from cyber security experts and from their friends and colleagues.

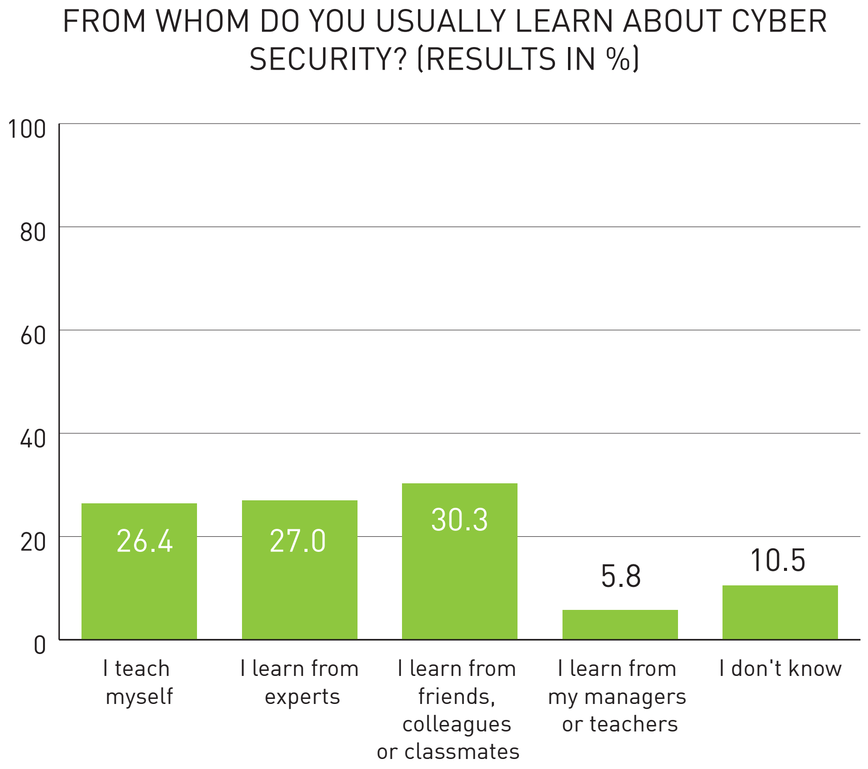


Figure 3: From whom do people learn about cyber security?

However, when we examine this more closely, we notice certain differences in how different groups learn about cyber security. Men teaches themselves more than women teaches themselves (36% vs. 18%), while women are more prone to seek advice from friends and colleagues than men are (36% vs. 24%)

Those under the age of 20 generally don't learn from experts, a mere 7% compared to the 27% in the general population.

Interest

Interests influences who we relate to and thereby who we learn from. While virtually everyone is positive towards new technology, only 47% are interested in technology and ICT.

We find that those who are interested in technology and ICT are more prone to learn by themselves (i.e. by trial and error) and from experts, while those who are not interested are prone to learn from friends and colleagues. Furthermore, those who are not interested in technology and ICT display a lower awareness about who they learn from. 19.3% say they don't know who they learn from, compared to 5.5% amongst those with such interests.

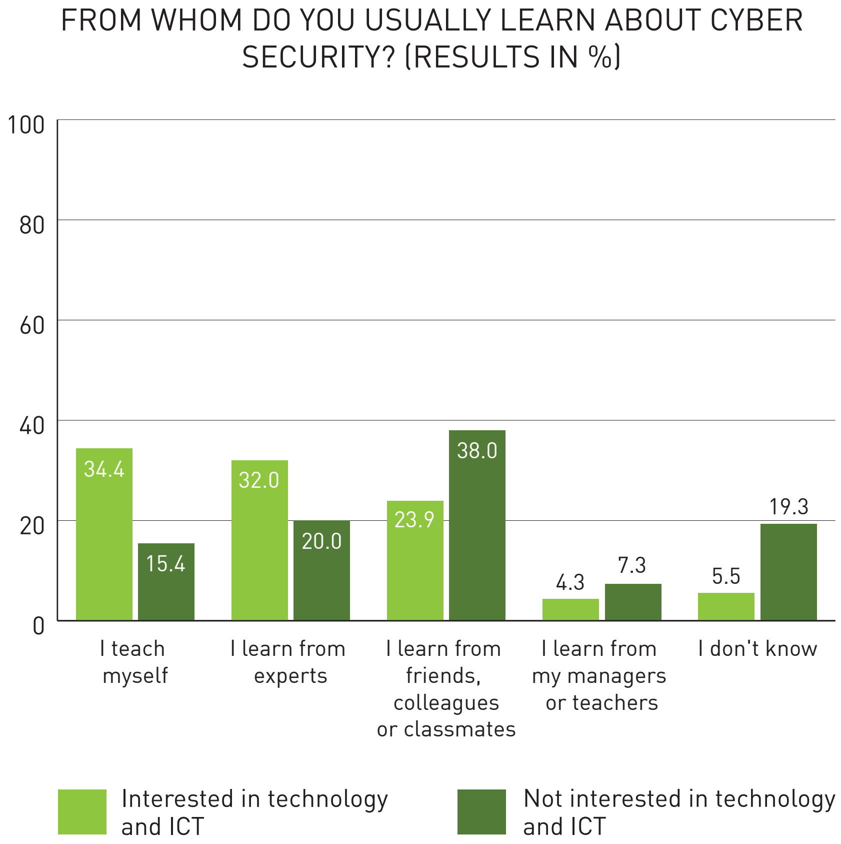


Figure 4: Source of learning vs. interest in technology.

Interest also plays a significant role in how we learn about cyber security. An interest in a topic will focus the attention, create curiosity, make us set aside time to explore the topic and make us accumulate knowledge in the area we are interested in. More knowledge may further develop the interest, and thus this becomes a self-enforcing loop. Our study shows that people who are interested in ICT are more prone to learn from trial and error, and by formal education, while those not interested are more prone to learn in an informal setting.

Assessment

Our study shows that only half of the general population have received cyber security education during the last two years, and that cyber security education is primarily a corporate effort.

It may come as no surprise that the elderly, in general, does not receive such education. This is a matter of concern because the elderly is indeed a part of our digital society. The Norwegian Directorate of Health reports[17] that the prognoses for the demographic development in Norway indicate a 15–20% increase in health costs during the 2010–2030 period. The Norwegian Directorate of eHealth[18] is a sub- ordinate institution of the Ministry of Health and Care Services, and its mission is to govern the use of tools and services using information- and communication-technologies that can improve the healthcare system as a whole, including increased patient safety, shorter health care waiting lists and reduced health care costs. eHealth is seen by many as a significant part of the healthcare challenges in the future, and that it may provide the elderly with better services, with a lower cost to the society. There is a concern that healthcare practitioners and those who receive healthcare services are unable to properly assess the risks associated with those services. Our study shows that the elderly is positive towards new technology, but only 37% of those above 66 years of age say that they feel capable to assess what is safe to do online. The introduction of new digital services, services that the society more or less impose on the elderly, presupposes a certain level of knowledge on how to navigate the digital landscape safely. Our study shows that the elderly is not given enough cyber security education. This may lead to security incidents where personal information is compromised, or where new eHealth systems and equipment are used in a way that may pose a danger to their wellbeing.

The situation for the group below 20 years of age is slightly better, even though less than a third has received cyber security education during the last two years. The young mostly learn about cyber security from their friends, and by try and error themselves. This indicates a more informal transfer of knowledge, and this poses a risk to the quality and accuracy of the knowledge they obtain. A study[19] (2014) by The Norwegian Media Authority shows that 88% of children between 1 and 12 years use the internet every week or more often, and 55% use it daily. The study concludes that more children use the internet than before, and the age-group 1–4 years increases the most.

[17]: https://helsedirektoratet.no/Lists/Publikasjoner/Attachments/73/Medisinsk-teknisk-utvikling-og-helsekostnader-en-gjennomgang-av-aktuell-kunnskap-IS-2142.pdf

[18]: https://ehelse.no/english

[19]: www.medietilsynet.no/globalassets/publikasjoner/2015/rapport_foreldre_smabarns_mediebruk_2014.pdf

Photo: Nina Solbakken

Considering that only half of the adult population has received cyber security training, it is to be expected that many children are not given proper guidance from their parents in this area. One might think that children are naturally computer-savvy, but there is no reason to believe that they are equipped with a natural ability to understand the dynamic digital threat landscape. Statistics (2015) from Slettmeg.no[20] show that 7826 people contacted them to get help with everything from online bullying, removing compromising pictures or to handle online fraud. Many of these are in the younger generations.

This study does not examine the depth or quality in the cyber security education or training that people are given. We do believe however, that the cyber security education, in large, fail to teach them the complex interaction between the individual and the whole of society. 3 out of 4 don't believe that having a secure computer makes the internet safer as a whole. This may be explained by a unilateral focus on securing the computer for personal reasons (i.e. to prevent loss of personal information), and not enough focus on how this is an important contribution to the security of national critical infrastructure. As personal computing devices are networked, a more holistic approach to "cyber hygiene" for the entire national infrastructure seems necessary in order to create a more resilient digital landscape.

[20] **20**: "*EraseMe*", a help-service provided by The Norwegian Centre for Information Security.

We believe that interest shapes our attitudes, our skills and our knowledge.

Interest plays a significant role in how people learn about cyber security, and who they learn from. Interest in technology and ICT correlates with a pattern where people learn from experts, and from their own trial and error. This can be seen as a positive self-enforcing method of learning, where interest, curiosity and knowledge drives one another in a way that separate the people who are interested from the ones that aren't. If so, we should be able to discern differences in what people know or how they behave. In the question of whether a secure personal computer contributes to a more secure internet, we observe no difference in the answers from the group of

people who are interested and the group that are not. However, people who are interested in technology and ICT are significantly more confident that they are able to assess what is safe to do online, compared to the group that are not interested (68.2% vs 53.3%). Furthermore, our study shows that people who are interested in technology and ICT exhibit more a secure behavioural pattern than the people who are not interested. We investigate cyber security behavioural patterns in a later chapter. From this, we conclude that interest is a significant force that not only shape how we learn about cyber security, but also from whom we learn. Interest drives people towards learning from experts, and thus towards a transfer of competence that, presumably, has a higher quality. Interest correlates directly with a more secure behavioural pattern.

Photo: Nammo

Risk perception

Introduction

Risk perception[21] refers to the judgement that people make about the characteristics and severity of a risk. We are concerned with risk perception in our study, because we are faced with safety or security dilemmas every time we go online. Threats can manifest themselves in many ways, but we fail to comprehend the complex digital chain of events that may cause us to become vulnerable. Should you open the e-mail attachment? Will your posture on digital surveillance by the authorities really make you more secure, or will it cause you to be more exposed to cyber criminals in the long run? Do you accurately assess the risk related to your online activities?

Cyber security professionals often claim[22][23] that people are lacking knowledge on cyber risks, or that they are naïve[24][25] and unaware.[26] In the wake of large security breaches, it is not uncommon to see it explained by "the human factor". People get blamed for making wrong choices, due to misinterpretation of the risk associated with their actions. In the wake of such incidents, we often see that educational programs and awareness campaigns are put in place in order to prevent future incidents.

Risks, especially complex risks which contains a considerable human element, can be based more on our personal judgement rather than scientific calculations. A risk judgement can be influenced by a large number of factors, each of them changing from day to

[21] http://heatherlench.com/wp-content/uploads/2008/07/slovic.pdf

[22] http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf

[23] http://blog.trendmicro.com/trend-micro-lack-security-awareness-reason-high-number-cybercrime-victims/

[24] http://www.welivesecurity.com/2016/01/29/businesses-still-naive-risks-cybercrime/

[25] http://www.fin24.com/Tech/News/Young-people-more-naive-on-cyber-security-20151006

[26] http://www.businessinsurance.com/article/99999999/

day, or situation to situation. Facts and knowledge may play a large part in the judgement, but so does experience, how "risky" we feel that day or if you generally are a risk-averse person or not. What are the factors that influence that judgement, and what do we do when we are faced with risk situations? If the goal is to enable people to make better risk judgements, how should we go about that?

In this study, we are interested in different aspects of risk perception, and what factors that correlates with risk perception.

Our findings

72.1% of the participants of this study thinks that they expose themselves to risk when they are online, and most people think that the threat is external, e.g. that someone will do something to them, rather than themselves doing something to compromise their online safety.

Table 2: Perceived largest online threat. N=8166

WHAT DO YOU THINK IS YOUR LARGEST ONLINE THREAT?	%
That you will do something yourself that compromises your online safety.	24.1
That someone else will do something to you (e.g. hack a site where you have some personal information)	67.8
I don't know	8.2

Before looking into how the participants perceive risks associated with online threats, we asked whether or not they feel capable of assessing what is safe to do online. 61.1% of the participants think that they are able to do that assessment, while 23.5% say they don't think they are able. 15.3% say they don't know whether they can assess that or not.

We chose a number of online threats that most people are, or can be, exposed to. These are online fraud, identity theft, online bullying or harassment, destruction of information, malicious code and manipulation. We then ask the participants to rate how worried they are that those threats will happen to them on a scale from 1 to 5, where

1 is “Not worried at all” and 5 is “Significantly worried. When presenting the results, we aggregate the responses 4 and 5 into a category we call “Worried” and the responses 1 and 2 into a category we call “Not worried”. The response 3 is called “Neutral” in the following presentation.

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?	Average (1–5)	Not worried %	Worried %	Neutral %	I don't know %
That my bank- or credit cards will be used in online fraud	3.5	20.2	51.3	27.1	1.4
That others will use my identity online	3.6	20.2	53.9	24.4	1.4
That I will be bullied or harassed online	2.3	61.1	17.2	19.6	2.2
That my digital documents or pictures will be destroyed or deleted	3.4	23.9	49.6	24.7	1.8
That a virus will infect my computer	3.6	19.0	56.5	23.2	1.3
That I will be manipulated to send sensitive information to someone	3.0	41.7	36.2	20.7	1.4

Table 3: Risk perception. n=8193

We create a visual representation of the average results, where a larger area means that the participants are more worried.

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?
(1: NOT WORRIED AT ALL. 5: SIGNIFICANTLY WORRIED)

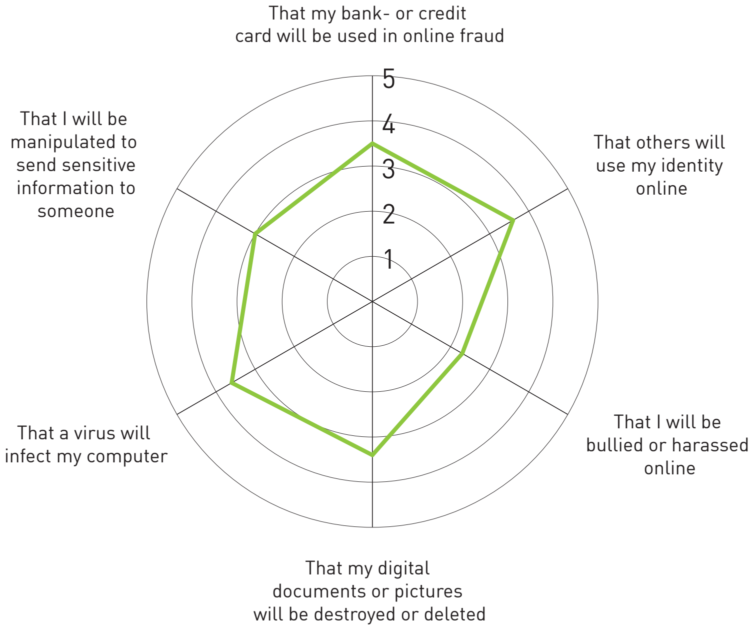


Figure 6: Average risk perception

Many cyber security educational programs aim to raise the awareness on digital threats. In this study, we do not find that those who had cyber security education during the last two years, perceive the threats differently than the group that did not have such education.

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?
(1: NOT WORRIED AT ALL. 5: SIGNIFICANTLY WORRIED)

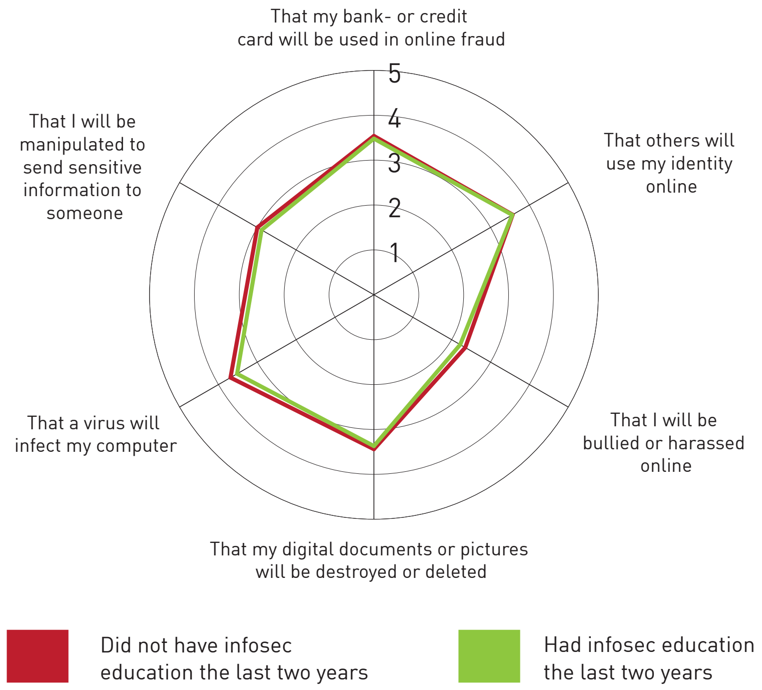


Figure 7: Average risk perception vs. Cyber security education

We do however observe a correlation between risk perception and confidence in the participant's ability to assess risk. In this study, we find that people who do not think that they can assess what is safe to do online are significantly more worried about the online threats.

This study has shown that an interest in technology and ICT plays a significant role in how and from whom people learn about cyber security. Interest could very well be a significant factor in how we perceive risk. However, we do not observe any significant differences between the group that is interested in technology and ICT, and the group that is not, with one exception. People who are not interested in technology and ICT are significantly more worried about malicious code (e.g. viruses) on their computer.

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?

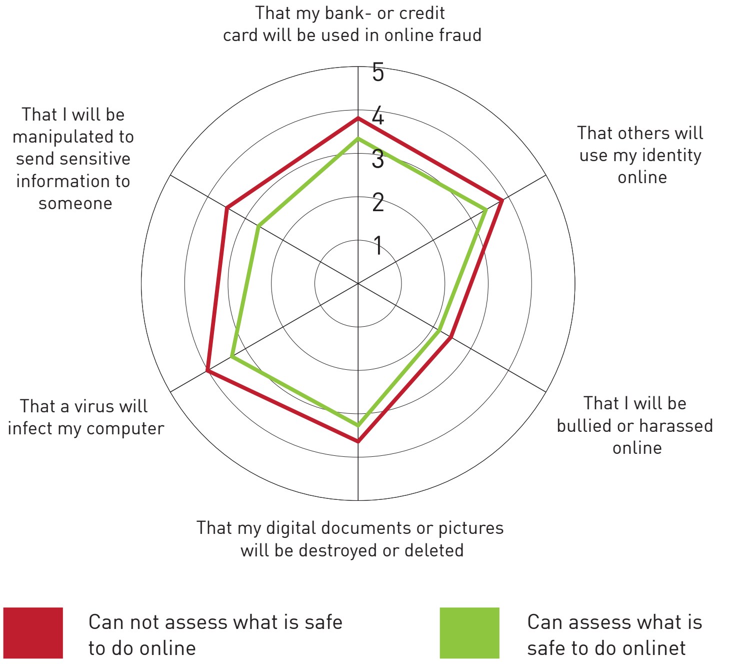


Figure 8: Average risk perception vs. Ability to assess what is safe to do online

Furthermore, we find that age also correlates with risk perception in this study. The older people are, the more they worry about the digital threats.

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?

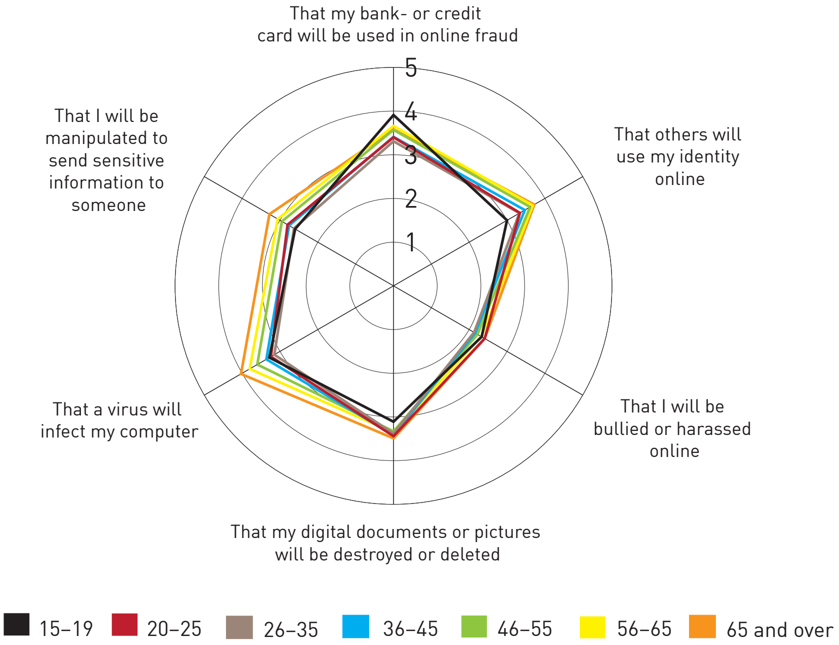


Figure 9: Average risk perception vs. Age

We also study how much risk the participants associate with activities most people engage in online. We ask the participants to rate how they perceive risk associated with the activities on a scale from 1 to 5, where 1 is “Not worried at all” and 5 is “Significantly worried. When presenting the results, we aggregate the responses 4 and 5 into a category we call “Worried” and the responses 1 and 2 into a category we call “Not worried”. 3 is coined “Neutral” in the following presentation.

Table 4: Risk perception in relation to online activities. N=8193

HOW WORRIED ARE YOU THAT THE FOLLOWING WILL HAPPEN TO YOU?	Average (1–5)	Not worried %	Worried %	Neutral %	I don't know %
Using online banking	2.06	70.8	10.0	10.0	2.1
Using email	2.52	51.2	18.2	18.2	1.2
Sharing passwords with others	4.49	6.2	85.0	85.0	2.5
Using the same password at several online services	3.75	11.6	61.2	61.2	2.0
Using bank or credit cards online	2.83	33.0	36.0	36.0	1.5
Using online gambling	4.13	7.7	45.8	45.8	39.0
Using social media	3.04	27.5	30.4	30.4	6.5
Not back-up your data	3.92	11.5	63.1	63.1	7.1
Using public (government) services online	2.26	61.0	12.6	12.6	4.2

We create a visual representation of the average results, where a larger area means that the participants associate more risk to the activities.

We find that cyber security education does not play a significant role in how people assess the risk associated with the online activities. When it comes to interest in technology and ICT, we find some significant differences. The participants that are interested in technology and ICT, associate more risk to not backing up data and to use the same password at several online services.

We find that the participants who don’t think they can assess what is safe to do online, associate significantly more risk to the online activities. However, when it comes to the more technical activities, which coincidentally also are activities that they control themselves, there are no significant difference between the two groups.

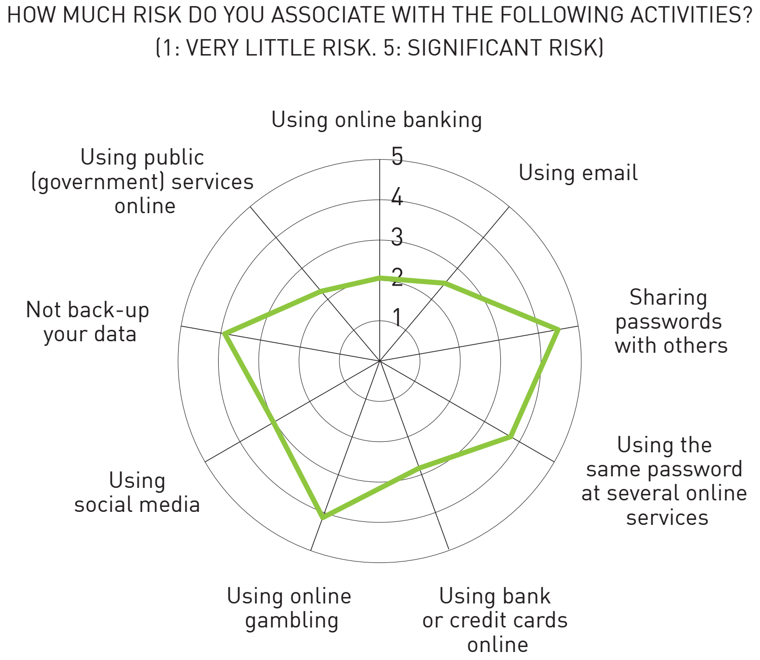


Figure 10: Average risk perception in relation to online activities.

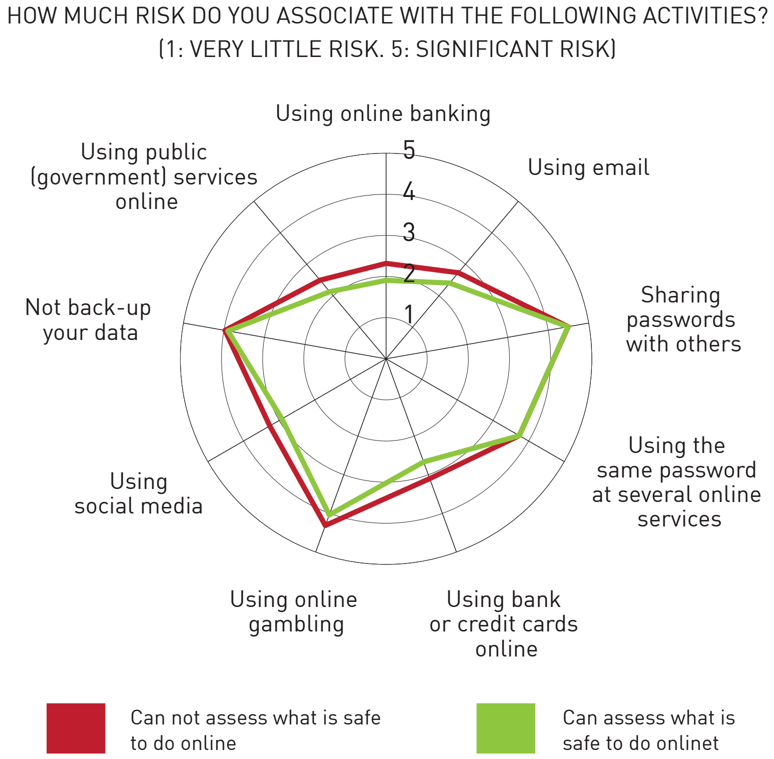


Figure 11: Average risk perception in relation to online activities vs. Ability to assess what is safe to do online

Assessment

The results are not interpreted according to their "correctness". Risk perception is subjective in its nature, and there are factors that are likely to skew how we perceive the risks we examine in this study. An online bank may appear solid because we "know" they have vaults and other security systems in place. Our feelings about how secure a bank is, may affect how we think about online banking. In the same way, online gambling could be seen as less safe because there is already quite a lot of risk involved with gambling in the first place.

It is still useful to examine risk perception and how it evolves over time, how it changes when security incidents occur and how it relates to other factors. This study, then, can be seen as a baseline study for digital risk perception, and we will be able to discern trends when using the method over time.

We learn that cyber security education does not significantly change how the participants perceive digital risks. These results seem to be in conflict with how many cyber security professionals view the purpose of such education. The general idea is that education, the transfer of facts, about threats and vulnerabilities, will enable the students' abilities to assess the risks. Subjective risk, however, is not based on careful calculations of facts and factors. Personal experiences, feelings, emotions and events in the recent past plays a much larger role in how we decide what risk we associate with different activities or threats. When cyber security education fails to affect how people perceive digital risks, the issue may very well be that the educational programs are using the wrong kinds of communicational methods or that the syllabus is inadequate.

We find that age correlates with risk perception, and that people worry more about digital risk as they get older. This may prove to be a troubling factor in the digitalization processes that are happening in both the private and public sector. The society expect the individual to be a part of the digital transformation, and how we perceive the risks associated with this transformation can affect the effectiveness of the transformation itself, or how we cope with it as individuals. If people think that some digital services are unsafe, they may very well refrain from using them. 44% of the participants in this study say that they have refrained from using an online service after they have learned about threats or security incidents. A recent study[27] by the US Department of Commerce National Telecommunications & In-

[27] https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

formation Administration corroborate these findings, and show that many Americans are deterred from engaging in important economic and civic online activities due to privacy and security concerns.

Risk perception also seem to be linked with how the participants think they can assess what is safe to do online. The people who think they can assess what is safe, tend to see online activities as riskier, though there are some exceptions. We find no differences when it comes to technical matters, such as not backing up their data, sharing passwords with others or using the same password on several online sites.

Behavioural patterns

Introduction

Cyber security behaviour practices and patterns has been subject to research and evaluation over a large period of time, and across different industries. Most efforts in this area are conducted within businesses, and the goal is to enforce, to them, a correct security practice in order to prevent security incidents that may affect the quality of products and hence business earnings.

Regardless if you are using ISO/IEC 27001/27002, COBIT, The Norwegian Security Act[28] or any internal cyber security framework or policy; the overarching goal is to set a standard for security behaviour and to implement controls to ensure that the employees are compliant.

Now, while these standards are perfectly fine for a company or organization, they are not necessarily useful in every part of the society. ISO/IEC 27002 is not designed to be used as guidelines for a family of four, in the classroom in high school or at the home for the elders. Still, we are all part of the digital society and we all take part in the national cyber security culture.

Standards set aside, cyber security professionals advocate certain behavioural patterns that they deem to be good. Although the behavioural patterns may be seen as normative, they will change over time because both the threat and how we use the technology changes.

[28] Lov om forebyggende sikkerhetstjeneste (LOV-1998-03-20-10)

For this study, we have chosen the core security practices that applies to both personal and business use of the internet. These are identity control and protection, safe online behaviour, keeping an updated computer system, data protection and the use of security systems.

At the end of the day, we want everybody to behave securely and to contribute to a safe digital landscape for everyone. However, we need to know more about how we can contribute and encourage everyone to develop safe and secure practices. Again, we find that cyber security education is the preferred tool to achieve this. But; does it work the way we intend to? What factors contribute to safe and secure practices?

Our findings

In our study we find that most people assess whether a website is safe before using it. Still, 18.1% say that they never assess how safe it is. We encourage frequent assessments due to the changing nature of cyber threats, but these findings must also be seen in the context of the competence and skills required to assess whether a website is safe. In this study, 61.1% report that they think they are able to make such an assessment.

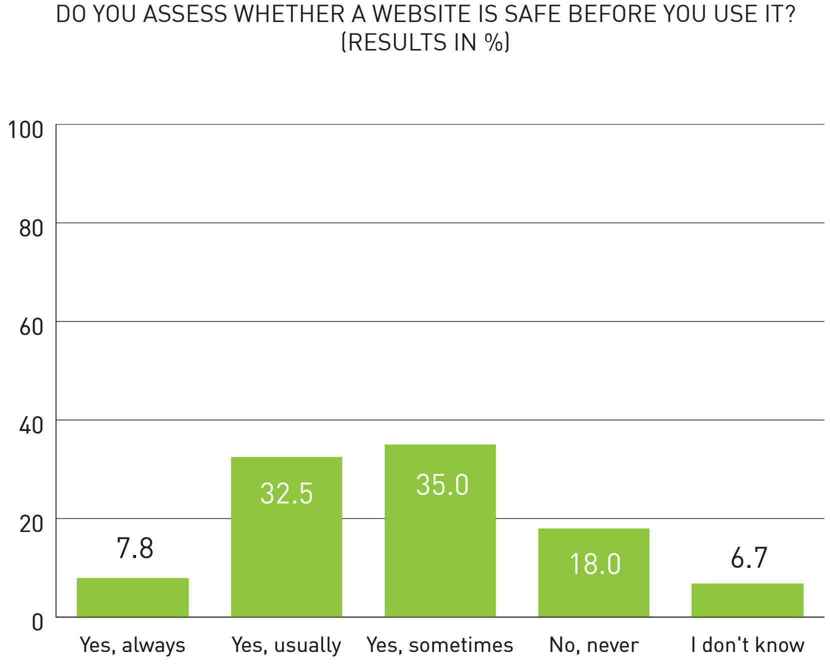


Figure 12: Assess whether a website is safe to use

It is common for businesses to lay out the rules for using ICT at the workplace. The rules typically include a more general code of conduct, as well as explicit cyber security regulations. We find that 85.3% of the participants that are employed know that their workplace has rules for cyber security. Only 4.7% say that their workplace does not have such rules, and 10% say they don't know whether the workplace has rules or not. The practice of bringing personal computer devices (BYOD) to work is trending, and we find that 32% say that they are allowed to use private equipment at work, while 45% say that they are not allowed.

Although most businesses implement cyber security rules, it is not to say that everyone will follow all the rules all the time. We find that 9.5% say that they sometimes deliberately break cyber security regulations. The study does not give answers to why they break the rules. However, if the rules are considered counterproductive and adversely affect the person's ability to do their job, people may "bend" them to improve their personal efficiency and effectiveness, despite them knowing the rules. Interestingly, we find that nearly twice as many deliberately break the rules in the private sector, then in the public sector, 14.1% in the private sector vs. 7.8% in the public sector. There is also a greater uncertainty to whether they break the rules in the private sector.

I SOMETIMES DELIBERATELY BREAK INFORMATION SECURITY REGULATIONS	Private sector, %	Public sector, %
Yes	14.1	7.8
No	64.7	74.9
I don't know	21.2	17.3
n=	**2213,0**	**3978,0**

Table 5: Deliberately breaking the cyber security regulations

Men deliberately breaks the cyber security rules more often than women, 13.8% vs. 5.6%. When we examine the different age groups, we learn that people over 55 are less likely to deliberately break the rules, and that the young are less aware whether they break the rules or not.

Table 6: Deliberately breaking the cyber security regulations vs. Age (Results in %)

I SOMETIMES DELIBERATELY BREAK INFORMATION SECURITY REGULATIONS	15–19	20–25	26–35	36–45	46–55	56–65	66 and above
Yes	16.9	12.2	16.1	12.4	15.2	5.3	5.3
No	36.6	50.6	61.9	72.6	50.2	75.7	67.8
I don't know	46.5	37.2	22.0	15.0	34.6	18.9	26.9
n=	**628.0**	**164.0**	**940.0**	**1576.0**	**855.0**	**1553.0**	**1324.0**

Passwords

Identity management and protection is a core element of a sound cyber security practice. Although new forms of identity management, such as biometric solutions, are made available, most digital services still rely on some form of password or code. Identity theft is often an integral part of online crime, and often we find that the password is the only thing that separates the criminal from achieving their goals. Password based security has been around for decades, but they still represent a significant challenge for both cyber security practitioners and everyone who use them. UK Government Communications Headquarters (GHCQ) and UK Centre for the Protection of National Infrastructure issued a Password Guidance[29] in 2015 where they state that UK citizens had an average of 22 online passwords. This is of course far more passwords than anyone can remember, especially if one is forced to change them at some interval and to construct them according to strict rules. We have no reason to believe that the numbers are any lower for Norwegian citizens.

We find that there is a balance where people can manage their passwords both efficiently and securely. This study focuses on a few core elements of a secure password practice, and these are the current recommendations that we base our study on: We recommend that efforts are made to create secure passwords, i.e. passwords that are easy to remember but hard for others to guess. Length is a factor, as well as adding complexity to the password. A line from your favourite song is far more secure than using your first name followed by your birth date. We also recommend that different passwords are especially created for each online service. This may prevent that all your digital assets are compromised if one of your online service is compromised. One common method is to add the name of the service to your carefully constructed password. Finally, we recommend password-managers. These are security systems that allows you to create long and complex passwords for each of the online services you use.

[29] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

Some may think that we are missing out a few advices, such as not writing the password down, or that you should change the password regularly. Many security policies explicitly enforce these as rules. However, we now recommend that you write your passwords down, and store the paper in a relatively safe environment. We also recommend that you don't change your password regularly because it is more likely to make you chose simpler and easier to guess passwords. There is one exception to the last advice though; If you suspect that an online service is compromised, change the password immediately.

In this study we find that people, in general, could have more secure password practices. Nearly one out of five use the same password everywhere, and more than one third of the participants say they try to create secure passwords.

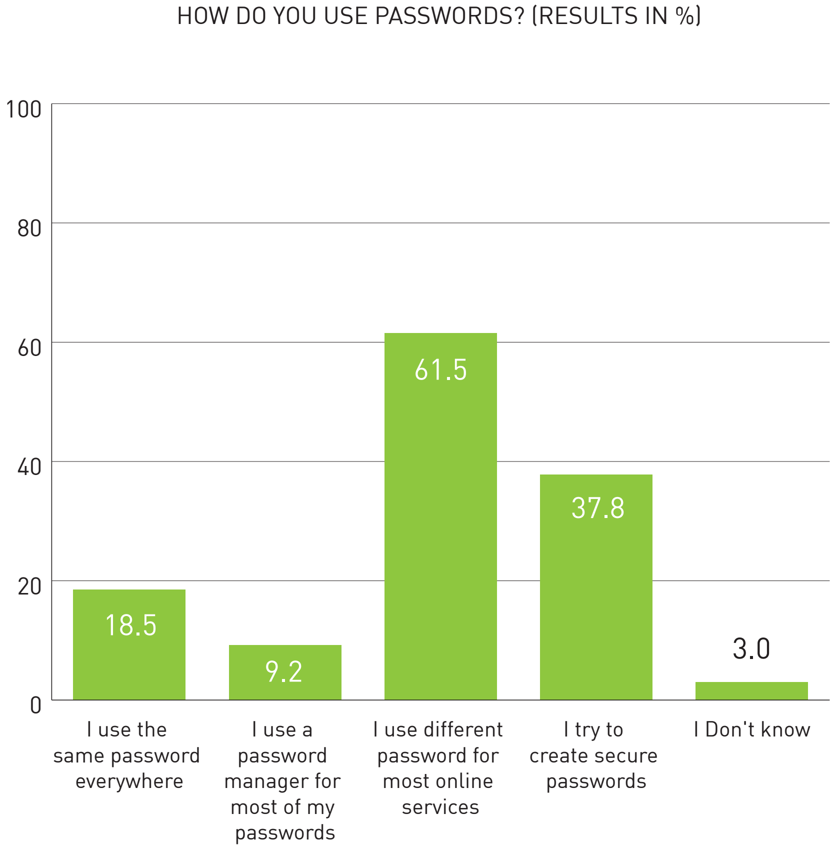


Figure 13: How people use passwords

When correlated with interest in technology and ICT, we find that significant better result for the group that have such interests.

Table 7: How people use passwords vs. Interest in technology

HOW DO YOU USE PASSWORDS?	Interested in technology and ICT, %	Not interested in technology and ICT, %
I use the same password everywhere	14.9	26.1
I use a password manager for most of my passwords	13.5	5.3
I use different password for most online services	66.1	52.6
I try to create secure passwords	44.9	27.2
Don't know	2.0	6.2
n=	**3855.0**	**1589.0**

When correlated with cyber security education, we find an improvement for the group that has received cyber security education during the last two years.

Table 8: How people use passwords vs. Cyber security education

HOW DO YOU USE PASSWORDS?	Has received formal information security training within the past two years	Has not received formal information security training within the past two years
I use the same password everywhere	14.7	21.1
I use a password manager for most of my passwords	10.8	7.8
I use different password for most online services	63.9	60.8
I try to create secure passwords	42.0	34.3
Don't know	2.0	3.0
n=	**4105.0**	**3647.0**

Cyber security software

Cyber security software are programs that monitor user behaviour or know threat activities, and that enforce technical security controls on the behalf of the user. Most are familiar with anti-virus and firewalls, but there are numerous other programs that can aid the user towards a more secure online experience.

We recommend that such programs are used according to the threat level, and that anti-virus and a personal firewall is a required minimum. Indeed, most modern operating systems today have such security software pre-installed.

We find that very few state that they don’t use any cyber security software at all.

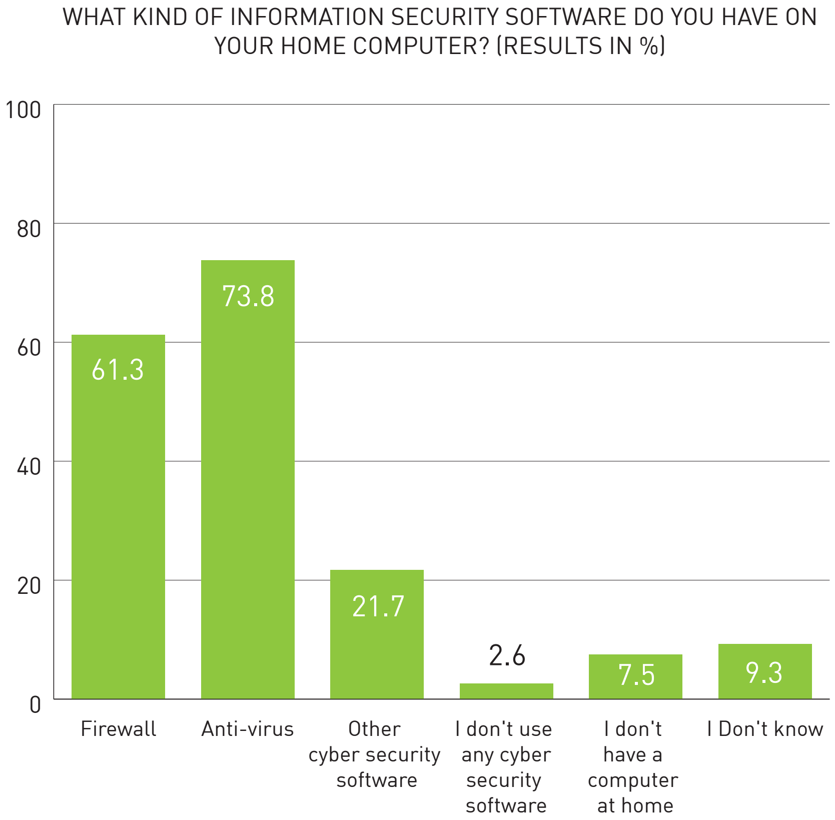


Figure 14: How people use cyber security software

Again, we find that an interest in technology and ICT plays a significant role when it comes to cyber security software.

WHAT KIND OF INFORMATION SECURITY SOFTWARE DO YOU HAVE ON YOUR HOME COMPUTER?	Has interest in technology and ICT, %	Has no interest in technology and ICT, %
Firewall	74.0	43.8
Anti-virus	80.3	62.1
Other information security software	28.1	13.4
I don't use any information security software	2.8	2.4
I don't have a computer at home	5.2	9.0
Don't know	3.9	22.2
n=	**3855.0**	**1589.0**

Table 9: How people use cyber security software vs. Interest in technology

However, we do not find that cyber security education during the last two years correlates with a better practice when it comes to using cyber security software. At a confidence level of 95%, we cannot conclude that there are any differences between the two groups.

WHAT KIND OF INFORMATION SECURITY SOFTWARE DO YOU HAVE ON YOUR HOME COMPUTER?	Has received formal information security training within the past two years	Has not received formal information security training within the past two years
Firewall	62.0	62.5
Anti-virus	74.3	75.5
Other information security software	22.9	20.6
I don't use any information security software	2.1	3.1
I don't have a computer at home	9.1	5.6
Don't know	7.4	9.2
n=	**4105.0**	**3647.0**

Table 10: How people use cyber security software vs. Cyber security education

Data protection

Norwegians are generally concerned with privacy, and we find that close to everyone say that they would erase personal information from their device if they were to sell it or throw it away. 90.6% say they would erase the personal information, while only 2.9% say that they would not erase it. 6.5% say that they don't know if they would erase it.

A large part of cyber security practices focuses on protecting data from unauthorized access, manipulation or to make sure that the data is available when it should be. Some digital threats, such as ransomware[30] can render the information useless to its owner, and having a back-up is in many cases the only remedy.

We find that 76% of the participant's back-up their data, and that most people do this less often than every month.

When we examine what factors that correlates with the use of back-up, we find that an interest in technology and ICT correlates with a more frequent use of back-up.

Furthermore, we find that an cyber security education during the last two years correlates with a more frequent use of back-up, although the effect appears to be weaker than for the group that is interested in technology and ICT.

[30] http://www.trend-micro.com/vinfo/us/security/definition/ransomware

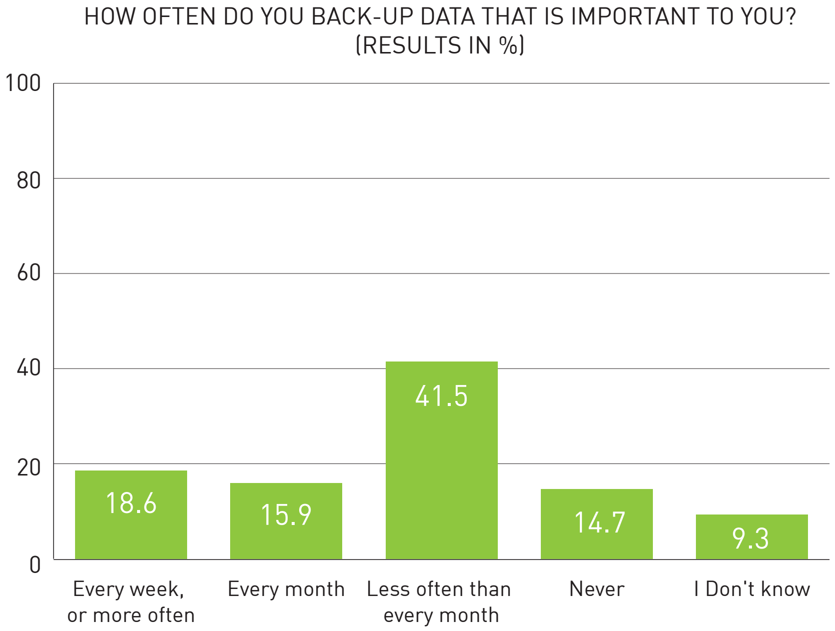


Figure 15: How people back-up their data

HOW OFTEN DO YOU BACK-UP DATA THAT IS IMPORTANT TO YOU?	Interested in technology and ICT, %	Not interested in technology and ICT, %
Every week, or more often	28.3	9.0
Every month	20.5	10.4
Less often than every month	38.7	44.8
Never	7.7	31.7
Don't know	4.8	4.1
n=	**3855.0**	**1389.0**

Table 11: How people back-up their data vs. Interest in technology

HOW OFTEN DO YOU BACK-UP DATA THAT IS IMPORTANT TO YOU?	Has received formal information security training within the past two years	Has not received formal information security training within the past two years
Every week, or more often	21.9	15.8
Every month	17.7	14.7
Less often than every month	41.7	42.4
Never	10.6	18.8
Don't know	8.1	8.2
n=	**4105.0**	**3647.0**

Table 12: How people back-up their data vs. Cyber security education

Assessment

For this study, we chose the core elements of what we believe is a good cyber security practice. We see these practices as normative, but we are also well aware that what we consider to be “best practice” will change over time. Furthermore, the norms may be different for different groups or for the activities involved. For example, we would generally advocate a frequent use of back-up, but if the information is updated less than every month, it makes little sense to spend time doing back-up every week.

There has been quite a lot of research, studies and experiments that focuses on cyber security behaviour patterns, but few look into the underlying factors that correlates with a better practice. Cyber security education is the preferred tool for most businesses, under the supposition that such education leads to a better practice. In this study, we find that people who had formal cyber security education during the last two years, exhibit a better practice than the ones that did not have such education. However, the effect is small, and in some areas we do not find any correlation between such education and a better practice.

This study does not evaluate the content or quality of the cyber security education that the respondents have received, but in general, our findings indicate that there is a need to look into these educational programs to assess their validity and effect.

We find a significantly stronger correlation between an interest in technology and ICT and a good cyber security practice. We believe that this must be seen in the context of how people learn about cyber security, where an interest in the field means that you learn more from experts and by setting aside time to learn from your own trials and errors.

Compliance to the cyber security rules are a concern for most businesses. Not everyone can be experts on current threats or the most effective counter-measures. The rules reflect the cyber security policy, and ultimately the goal of the business. We find that most people follow the rules, but that the number of people who don't know if they break the rules or not are quite high. This could mean that businesses to some degree fail to communicate to its employees what the rules are, or that the rules are seen as irrelevant or inept.

Knowledge on how to assess what is safe to do online is essential to avoid manipulation and other criminal activities.

The threats are constantly evolving, and what was safe yesterday may not be safe today. The group that either do not assess whether a website is safe before using it and those who don't know, amounts to nearly 25%.

The technical advances are taking over some of the burden of keeping us safe online. More and more devices now come with encrypted filesystems, reducing the need to erase the data when the device is sent away. ICT eco-systems comes with integrated cloud-based back-up solutions. Biometrics are taking over from passwords. All these advances are indeed creating a more secure technical environment; still cybercrime is on the rise.[31] When the cyber criminals are turning away from attacking the device, to attacking the humans, the ability to assess what is safe to do online becomes more important. Hence, this should be a prioritized area if we are to increase our national digital resilience.

[31] **31**: http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/cybercrime.html

TANNLEGE

Main conclusions

Even though cyber security education is not a panacea, we find that it correlates with behavioural patterns; that is, people who are educated in cyber security, acts more securely online. Still, our findings indicate that there is a great potential for improvement in how the Norwegian population is educated in this field. The government is not taking proper responsibility to educate its citizens, hence it is left to the businesses. The problem with this is apparent: A huge part of the population is left out. The young, the old and the people who for some reason aren't part of an organization that provide them with cyber security education. Furthermore, the logic in a business differs from the logic of a nation. The focus on compliance to the business' internal security policies is of course helpful, but it is more than likely that it will not enable the individual to become more resilient to online fraud, cyber bullying and other unwanted or criminal activities that takes part outside of the businesses area of interest.

There is a need for a stronger commitment from the government to ensure that the whole population is properly educated in cyber security. By implementing such education early in the schooling system, one can hope to instil an interest in cyber-related matters into the young. They may seem techno- savvy, but it is necessary to ensure that what they are taught is correct and current. This study has shown that very few under the age of 20 has been educated in cyber security, and those who have knowledge, have learnt from each other rather than from experts in the field.

At the other end of the age range, we find similar facts. The elderly is not being educated in cyber security, but we lay it upon them to take part in the digitalization of our society. The result is fear of what might go wrong. Furthermore, we know that fear of cyber incidents, such as hacking, can cause people to refrain from using the online services. We fear that the ongoing digitalization in the health care sector can experience a cooling effect due to lack of education.

Interest is a factor that correlates, rather strongly, with cyber attitudes, risk perception and behavioural patterns. This may seem obvious, because an interest in a certain topic will indeed make us spend time exploring it, seeking knowledge and learn more about it. Even though almost half of the population claims to be interested in technology and ICT, there is still a larger percent that is not. We don't believe that we can make someone interested, but we surely can make cyber security more interesting. We find that many subject matter experts, news-sites, educational programs and other available information takes on a technical language and terminology that is more suited to alienate than to instil interest. When the method of communication is more customized to those not interested in technology and ICT per se, we think that this will enable them to see why this subject matters to them as well.

Not surprisingly, cyber governance and control has been debated for years. The discourse is carried out along several topics, where the matter of who and how power should be exercised online is probably the most engaging. The discussions are often polarized, where on one side, we find the governmental agencies who seek out wider mandates and better methods to fight crime and foreign intelligence services. On the other side of the argument, we find privacy concerns. We strongly believe that cybercrime should not be treated any different from other types of criminal activity. The police are given mandate to exercise power in our society, and should do so in the cyber domain as well. We find that people agrees with this in principal, but not in practice. Almost everyone wants to report online crime to the police, but less than half think that they will get help. A mere 13%[32] of the people who are subject to cybercrime, actually files a police report. Concurrently, 4 out of 10 say that activist groups indeed play a role in the fight against cybercrime.

[32] The Norwegian Police Citizen Survey 2015 - https://www.politi.no/vedlegg/lokale_vedlegg/politidirektoratet/Vedlegg_3493.pdf

This may forewarn an unwanted development, where people are taking matters into their own hands. We have seen this already, where activist groups go after criminal networks,[33] and that journalists[34] and individuals[35] are doing what we expect the police to do. At the core of this, we find a paradox: We expect the police to protect us, and at the same time, we refuse them the tools to do so. We do not believe that this is a simple matter of only giving the authorities the tools they want. The public need to see results in the cases that should and could be solved with the tools already available to them. Unless the public experience that the police can solve cyber-crime, we fear that the attitude on who that really exercise power in the cyber domain will further shift from the police, towards activist groups and individuals.

In order to protect the digital society as a whole, the individual must look beyond themselves. We find that there is a gap between what we expect people to do in order to protect themselves online, and what they actually do. This is obviously a matter of risk to the individual, but it is also a risk to the nation. Unsecured computers are valuable assets to criminal organizations, who infiltrate and use the computing power to attack critical infrastructures, businesses and other individuals. We find that few are aware of the impact their own neglect can have on the national cyber hygiene. We believe that this comparable to the use of vaccines in medicine. For them to be effective, a large enough group of the population must be vaccinated. In the same way, in order to disrupt the criminal value-chains, enough computers must be secure. We believe that our national resilience to cyber-crime will greatly benefit from a cyber security culture where the individual takes more responsibility for the security of the collective they are a part of and that they are assured help if they experience online crime.

[33] **33**: Anonymous "*Operation Death Eaters*" where they were collating evidence against international paedophile rings and their severe abuse of children to bring them to justice

[34] **34**: http://www.vg.no/spesial/2015/nedlasterne/

[35] **35**: http://www.ba.no/nyheter/nett-truslene/politi/dataekspert-mener-politiet-lett-kunne-sporet-avsenderen/s/5-8-151849

MH 4

Strategic policy advice

Our findings clearly show that actions must be taken to address the challenges, and that there is a need for a comprehensive approach that involves the government, governmental agencies, businesses, organizations and individuals. However, the government should take a leading role to ensure an efficient and unified approach. Based on our conclusions, NorSIS presents the following strategic advice:

1.

This study clearly shows that far too few are given cyber security education, and that current education does not have sufficient effect.

While businesses and organizations take responsibility to educate their employees, the young, the old and those unemployed are mostly left to their own devices. 71.6% of those under 20 has not received cyber security education during the last two years. For the elderly, those above 66, the situation is even worse: Only 17.5% has received such education.

Furthermore, we find that cyber security education that is given today does not lead to a significantly better security practices. 9.5% say that they sometimes deliberately break cyber security regulations, and as much as 22.6% say they don't even know what the rules are.

When correlated with cyber security behavioural patterns or with risk perception we find that the current cyber security education only has a small effect, and in some cases, no effect at all. We do however find a strong correlation between an interest in technology and cyber security practices. The fact that people who already are interested in technology performs better, is a clear indication that the cyber security education itself is technology oriented. Consequently, the cyber security education is perceived as inadequately by a large proportion of the citizens. In order to properly educate the Norwegian citizenry in cyber security, one must look to other educational methods and perspectives as well as other ways to reach those who are not employed by a business that provides such education.

We recommend that The Norwegian government should take greater responsibility for the cyber security education of its citizenry, especially for the young, the old and those who are not employed. In addition to this, the government should stimulate both private and public sector to increase their efforts to educate their employees in cyber security. NorSIS recommend that the government device a strategy for cyber security education based on the following principles:

a. We believe that cyber security culture can be shaped early in life, and that it can result in a more resilient cyber hygiene for our nation. The government should increase its effort to educate the young in cyber security. Children are presented with technology at a very young age, and there is a need to make it a priority to ensure that the young not only are taught how to use technology, but also how they shall conduct themselves safely and securely online. NorSIS recommends that the government approaches this challenge comprehensively. Surely, the school system should play a key role in educating the young, but other possibilities, such as private- public endeavours, non-governmental organizations and voluntary initiatives, can also play an important role.

b. The government should apply targeted education programmes to ensure that specific groups are given competence on how to conduct themselves safely and securely online. These programs should be aligned with the digitalization strategies, to make sure that individuals that are affected by the digitalization are included into the programs. As an example, the digitalization of the health care sector may require cyber security education programs customized for the users of such technology.

c. The government should stimulate businesses and organizations in order to encourage them to take greater responsibility for providing cyber security education to their employees. We believe that public private partnership and economic incentives for cyber security education will improve national cyber hygiene significantly.

2.

The trust that the Norwegian citizenry place in the law enforcement agencies ability to handle cyber-crime is fragile, and we face a situation where vigilante justice become prevalent.

It is vital that the Norwegian citizenry have trust in the government and governmental agencies, especially in the matter of exercising power. It is of utmost importance that the government ensures a rule of law, and prevent online vigilante justice. Our study, corroborated with reports from the law enforcement agencies, indicated that this trust is limited. 85.6% say that they will report online fraud to the police. For identity theft, even more say they will: 92.9%. However, only 45.8% thinks that the police will be able to help them if they are subject to cyber-crime. The police themselves report that only 13% of the people who are subject to cyber-crime actually files a police report. At the same time, an alarming 41.1% say that they think that activist groups and individuals should play a part in the fight against such crime. This shows a tendency where groups and individuals increasingly take the law into their own hands in absence of effective law enforcement.

Cyber security will always be a public private endeavour, but online law enforcement is a clear government responsibility. Today Norwegian citizens evaluates this responsibility to be deficient attended by the police. NorSIS recommend that the police must be properly educated, equipped and trained to prevent and investigate cyber-crime. Furthermore, they should be required to prioritize cyber-crime in order to ensure jurisprudence also for this type of crime. NorSIS recommend that these indicators are observed over time in order to discern changes in the trust that the Norwegian population places in governmental agencies in this matter.

The protection from online harassment and abuse can sometimes be found in the grey area between criminal activity, unfortunate circumstances and legal activity. Cyber-crime and online harassment and abuse can affect the population randomly and with a broad impact. We believe that non-governmental organizations should play an important and necessary role in offering free and independent help and assistance to handle online harassment, abuse and crime.

3.

The Norwegian citizenry are not aware of how their neglect in cyber security affects the resilience of the entire national digital infrastructures.

The future national cyber security should build upon a wider knowledge of cyber- immunology. The overall resilience will be significantly dependent on the actions of the individuals, much like vaccine theory in medicine. Our study shows that the awareness on how the individual impacts the resilience of the entire digital landscape, is low. Only 15.6% say that they think that the internet becomes more secure if their own computer is secure. Security measures and educational programs are often narrowly scoped and stow piped. They mainly focus on the direct reduction of the individual's exposure to risk. As presented in the Official Norwegian Report 2015:13 "Digital vulnerability – safe society",[36] national critical infrastructures and services, and indeed most of our gross domestic product, are made possible due to "long value chains" that spans many sectors, businesses and agencies. Good cyber security initiatives are plentiful, but they mostly exist in isolation. In order to achieve a truly holistic approach to our national challenges, NorSIS recommends that The Ministry of Justice and Public Security creates a national cyber security advisory board. This should be created as a private-public endeavour to ensure the participation of all relevant sectors, businesses and agencies.

4.

This study show that it is possible to develop new and useful knowledge about the Norwegian cyber security culture. We are confident that we will be able to develop further insight if this method is applied over time. Specifically, we think that we will be able to discern attitudes and opinions before they are expressed as behavioural patterns. If this is the case, the government may be able to implement corrective measures in time before an unwanted situation arises. Thus, we recommend that The Ministry of Justice and Public Security tasks NorSIS with yearly cyber security culture surveys.

[36] https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

NorSIS
Norsk senter for
informasjonssikring

Norwegian Centre for Information Security is an independent, expert, non-profit organization committed to promoting awareness and effective cyber security measures, practice and policy. We informs on cyber threats, advice people violated online, and facilitate activities and events promoting effective cyber security practice.

NettVett.no

Free online service giving practical advice on cyber security and netiquette to Norwegian residents and SMEs

slett meg.no

Free advisory service for those who feel offended or experience violation of rights online

security divas

Network of women working for a safe and secure internet and appropriate cyber security policies

Nasjonal sikkerhetsmåned

Annual national campaign to raise attention on cyber threats and effective cyber security practices

NorSIS employees have broad knowledge and experience in cyber security. Our primary audience is small and medium size enterprises and Norwegian residents. We cooperate with enterprises in both public and private sector to increase knowledge on sound cyber security practice, motivate enterprises to take social online responsibility and improve national cyber resilience. Through a network of experts NorSIS produces, analyses and disseminates knowledge on cyber security and the cyber security culture.

Photo: Marine Harvest

Acknowledgements

A project of this magnitude requires different perspectives and competences. NorSIS has been fortunate to work with the best in the field. Still, none of this would have been possible without the support from The Ministry of Justice and Public Security, who has funded a large part of this project.

Project manager: Bjarte Malmedal (NorSIS)

The project established a reference group, consisting of cyber security professionals from relevant partners of NorSIS:

- Roar Thon, The Norwegian Security Authority (NSM)
- Bjørn Stærk and Kjersti Rønholt, The National Criminal Investigation Service (KRIPOS)
- Nils Kalstad Svendsen, The Norwegian University of Science & Technology (NTNU Gjøvik)
- Arne Røed Simonsen, The Norwegian Business and Industry Security Council (NSR)
- Johan Nygård, The Norwegian Centre for ICT in Education (Senter for IKT I utdanningen)
- Torbjørn Kveberg, The Norwegian Defence Research Establishment (FFI)
- Kirsi Helkala, The Norwegian Army Cyber College (FIH)
- Hilde Widerøe Wibe, The Business Association of Norwegian Knowledge and Technology Based Enterprises (Abelia)

- Caroline Ringstad Schultz and Britt Eva Bjerkvik Haaland, Agency for Public Management and eGovernment (Difi)

NorSIS is grateful for their time and effort to ensure the quality of the project.

Our approach in this project demands a competence that is hard to find among cyber security professionals. The Norwegian Cyber Forces made a contribution in kind, to let one of their researchers in the field of culture to work with us on the project.

Finally, we thank the 29 companies and organizations who allowed us to forward our questionnaire to a staggering 150.000 employees, members and customers.

Method development, analysis and report production by Hanne Eggen Røislien (Ph.D., Norwegian Cyber Forces) and Bjarte Malmedal (M.Sc., NorSIS).

Appendix A – Norwegian Questionnaire

Takk for at du deltar i denne undersøkelsen om informasjonssikkerhetskultur. Resultatet fra undersøkelsen skal brukes til å gi råd om en tryggere digital hverdag for alle.

Undersøkelsen tar 8-9 minutter. Besvarelsene er helt anonyme og kan ikke spores tilbake til deg.

Først vil vi vite litt om hvem du er.

1) * Kjønn

○ Kvinne
○ Mann

2) * Alder

○ Under 15
○ 15-19
○ 20-25
○ 26-35
○ 36-45
○ 46-55
○ 56-65
○ 66 og over

3) * Hva er ditt høyeste utdanningsnivå?

○ Grunnskole
○ Videregående skole
○ Universitets- og høgskolenivå lavere grad
○ Universitets- og høgskolenivå høyere grad
○ Annet
○ Ønsker ikke å svare

4) * Arbeider du i privat eller offentlig sektor?

○ Privat
○ Offentlig
○ Er ikke i arbeid

5) * Hvor bor du?

○ Østfold
○ Akershus
○ Oslo
○ Hedmark
○ Oppland
○ Buskerud
○ Vestfold
○ Telemark
○ Aust-Agder
○ Vest-Agder
○ Rogaland
○ Hordaland
○ Sogn og Fjordane
○ Møre og Romsdal
○ Sør-Trøndelag
○ Nord-Trøndelag
○ Nordland
○ Troms
○ Finnmark

6) Hvor mange ansatte er det i din bedrift?

○ Under 10
○ 11-25
○ 26-50
○ 51-100
○ 101-250
○ Over 250

7) * Hvilke radiostasjoner lytter du mest til? (Du kan krysse av flere)

□ NRK P1
□ NRK P2
□ NRK P3
□ Radio Norge
□ P4

□ P5
□ Radio 1
□ Annet
□ Lytter ikke på radio
□ Vet ikke

8) * Hvilke nettaviser leser du mest?
(Du kan krysse av flere)

□ Aftenposten
□ VG
□ Dagbladet
□ Nettavisen
□ Dagens Næringsliv
□ Teknisk Ukeblad
□ ComputerWorld
□ Digi.no
□ Wired
□ SeHer.no
□ Lokalaviser
□ Andre
□ Leser ikke nettaviser
□ Vet ikke

Våre verdier påvirker våre holdninger og meninger. Vi spør derfor om hvilken partitilhørighet du har.

Det er valgfritt å svare på dette, og vi minner om at undersøkelsen er helt anonym og kan ikke spores tilbake til den enkelte.

9) Hva ville du stemt dersom det var stortingsvalg idag?

○ Ønsker ikke å svare
○ Arbeiderpartiet
○ Fremskrittspartiet
○ Høyre
○ Kristelig Folkeparti

○ Miljøpartiet De Grønne
○ Senterpartiet
○ Venstre
○ Sosialistisk Venstreparti
○ Rødt
○ Annet parti
○ Har ikke stemmerett
○ Vet ikke

I denne delen stiller vi deg noen spørsmål om hvordan du ser på trygg nettbruk i et samfunn der teknologi blir stadig viktigere.

10) * Hvor enig er du i følgende påstander?

	Helt uenig	Delevis uenig	Delvis enig	Helt enig	Vet ikke
Jeg er positiv til å ta i bruk ny teknologi	○	○	○	○	○
Jeg vet hva informasjonssikkerhet er	○	○	○	○	○
Jeg utsetter meg selv for risiko når jeg bruker internett	○	○	○	○	○
Jeg synes at jeg får tilstrekkelig informasjon om de truslene som finnes på internett	○	○	○	○	○
Det er greit at min aktivitet på internett blir overvåket dersom det fører til at jeg blir tryggere på nett	○	○	○	○	○
Politiet vil hjelpe meg dersom jeg blir utsatt for datakriminalitet	○	○	○	○	○
Det bør være mulig å være anonym på internett	○	○	○	○	○

Internett blir ikke tryggere selv om min datamaskin er sikker	○	○	○	○	○
Jeg har tillit til at myndighetene sikrer informasjonen de har registrert om meg	○	○	○	○	○
Aktivistgrupper (f.eks. Anonymous) har en rolle i kampen mot datakriminalitet og cyber-krig	○	○	○	○	○

11) * Det hender at jeg bevisst bryter regler for informasjonssikkerhet

○ Ja
○ Nei
○ Vet ikke

12) Føler du deg i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett?

○ Ja
○ Nei
○ Vet ikke

13) Opplever du at det er tryggere å handle på norske eller utenlandske nettsteder?

○ Norske nettsteder er tryggere
○ Utenlandske nettsteder er tryggere
○ De er like trygge/utrygge
○ Det avgjørende er om nettstedet er velkjent
○ Vet ikke

14) Hvor synes du at det er viktigst å tenke på informasjonssikkerhet?

○ Hjemme
○ På jobb eller på skolen
○ Det er like viktig begge steder
○ Det er ikke viktig noen steder
○ Vet ikke

"Informasjonssikkerhet" er et begrep som viser til hvordan vi beskytter informasjon som er viktig for oss. I delen som kommer nå lurer vi på hvordan du forholderdeg til ulike trusler.

15) * Hvor bekymret er du for at det følgende skal hende deg?
(1: Ikke bekymret for at dette skal skje. 5: Svært bekymret for at dette skal skje)

	1	2	3	4	5	Vet ikke
At mine bank- eller kredittkort skal bli misbrukt på nett	○	○	○	○	○	○
At andre skal utgi seg for å være meg på internett	○	○	○	○	○	○
At jeg skal bli hetset eller mobbet på nett	○	○	○	○	○	○
At mine digitale dokumenter og bilder skal bli ødelagt	○	○	○	○	○	○
At jeg skal få virus på min datamaskin	○	○	○	○	○	○
At jeg skal bli lurt til å gi fra meg sensitiv informasjon	○	○	○	○	○	○

16) * Hvor stor risiko forbinder du med følgende aktiviteter?
(1: Svært lav risiko. 5: Svært høy risiko)

	1	2	3	4	5	Vet ikke
Bruke nettbank	○	○	○	○	○	○
Bruke epost	○	○	○	○	○	○
Dele passord med andre	○	○	○	○	○	○
Bruke samme passord på flere nett-tjenester	○	○	○	○	○	○
Bruke bank- eller kredittkort på nett	○	○	○	○	○	○
Nettgambling	○	○	○	○	○	○
Bruke sosiale medier	○	○	○	○	○	○

Å ikke ta sikkerhetskopi	○	○	○	○	○	○
Bruke offentlige tjenester på nett	○	○	○	○	○	○

17) * Hva er det sannsynlig at du vil gjøre dersom det følgende skjer deg?

	Ikke gjøre noe	Ordne opp selv	Få hjelp av en ekspert	Anmelde det til politiet	Vet ikke
Du blir hetset på internett	□	□	□	□	□
Du blir utsatt for nettsvindel	□	□	□	□	□
Du får virus på datamaskinen hjemme	□	□	□	□	□
Du blir utsatt for IDtyveri	□	□	□	□	□

18) Har kunnskap om trusler eller hacking noen gang fått deg til å la være å bruke en nett-tjeneste?

○ Ja
○ Nei
○ Vet ikke

19) Hva mener du er den største risikoen på nett?

○ At du selv skal gjøre noe feil
○ At noen andre skal gjøre noe mot deg (feks hacke en nettside hvor du har lagt inn personlig informasjon)
○ Vet ikke

Interesser, kunnskap og atferd henger gjerne sammen. Vi vil nå spørre deg om hva du er opptatt av, og hvordan du skaffer deg kunnskap om informasjonssikkerhet.

20) * Hvor interessert er du i teknologi og IT?
(1: Svært lite interessert. 5: Svært interessert)

○ 1
○ 2
○ 3
○ 4
○ 5
○ Vet ikke

21) * Kan du mer eller mindre om informasjonssikkerhet i forhold til resten av befolkningen?

○ Jeg kan mer enn gjennomsnittet
○ Jeg kan mindre enn gjennomsnittet
○ Jeg kan omtrent det samme som gjennomsnittet

22) * Hvem lærer du mest om informasjonssikkerhet av?

○ Jeg lærer meg selv
○ Eksperter
○ Sjefer eller lærere
○ Venner, kolleger eller klassekamerater
○ Vet ikke

23) Hvordan lærer du vanligvis om informasjonssikkerhet?

○ Prøver og feiler selv
○ Kurs eller utdanning
○ Hører om ting fra andre i en mer uformell situasjon
○ Vet ikke

24) * Har du fått opplæring i informasjonssikkerhet i løpet av de siste to årene?

○ Ja
○ Nei
○ Vet ikke

25) * Har arbeidsplassen eller skolen din regler for informasjonssikkerhet?

○ Ja
○ Nei
○ Vet ikke

25) * Har arbeidsplassen eller skolen din regler for informasjonssikkerhet?

○ Ja
○ Nei
○ Vet ikke

27) Synes du at du har fått bedre ferdigheter etter opplæringen i informasjonssikkerhet?

○ Ja
○ Nei
○ Vet ikke

28) * Hvilken sikkerhetsprogramvare har du på din private datamaskin? (Kryss av alle du bruker)

□ Brannmur
□ Anti-virus
□ Annen sikkerhetsprogramvare
□ Bruker ingen sikkerhetsprogramvare
□ Har ikke privat datamaskin
□ Vet ikke

29) * Undersøker du om en nettside er trygg før du bruker den?

○ Ja, alltid
○ Ja, som regel
○ Ja, av og til
○ Nei, aldri
○ Vet ikke

For dette spørsmålet tenker vi primært på hvordan du bruker passord i privat sammenheng, ikke på jobb.

30) * Hvordan bruker du passord?
(Du kan krysse av flere)¨

□ Jeg bruker samme passord over alt
□ Jeg bruker et passordverktøy for å hjelpe meg å håndtere ulike passord
□ Jeg bruker forskjellige passord for de fleste tjenestene på nett
□ Jeg legger vekt på å lage sikre passord
□ Vet ikke

For dette spørsmålet tenker vi primært på hvordan du bruker passord i privat sammenheng, ikke på jobb.

31) * Hvor ofte sikkerhetskopierer du data som er viktige for deg?

○ Hver uke eller oftere
○ Hver måned
○ Sjeldnere enn hver måned
○ Aldri
○ Vet ikke

32) * Hvis du skulle selge eller kaste en privat datamaskin, ville du da sørget for at alle personlige data blir slettet?

○ Ja
○ Nei
○ Vet ikke

33) * Har du rutiner for å oppdatere operativsystemene og programmene på din private datamaskin?

○ Oppdateringene skjer automatisk
○ Jeg oppdaterer med én gang de er tilgjengelige
○ Jeg har ingen rutiner for å oppdatere
○ Vet ikke

34) Har du kommentarer eller innspill til denne undersøkelsen?

Appendix B – English Questionnaire

Thank you for participating in this survey on cybersecurity culture. The results will help us to provide advice on how to create a safer online experience for everyone.

The survey takes about 8-9 minutes.

First, we would like to know a few general facts about you

1) * Sex

○ Female
○ Male

2) * Alder

○ Under 15
○ 15-19
○ 20-25
○ 26-35
○ 36-45
○ 46-55
○ 56-65
○ 66 and above

3) * What is your education level?

○ Primary school
○ High school
○ College (Bachelor's degree or similar)
○ University (Master's degree or above)
○ Other
○ I choose not to answer

4) * Are you employed in the pyblic or private sector?

○ Private
○ Public
○ I am unemployed

5) * What kind of area do you live in?

○ Rural
○ Suburban
○ Urban
○ Metropolitan

6) What is the number of employees at your workplace?

○ Under 10
○ 11-25
○ 26-50
○ 51-100
○ 101-250
○ Above 250

7)* What kind of radio stations do you listen to regularly? (You can choose more than one)

□ News radio
□ Music radio
□ Talk oriented radio
□ Local radio stations
□ National public radio
□ Commercial radio
□ Community radio
□ Other
□ I don't listen to radio
□ I don't know

8) * What kind of online news-sites do you visit regularly? (You can pick more than one)

□ Traditional news-sites (e.g. The New York Times)
□ Technology news (e.g. Ars Technica or Wired)
□ Lifestyle Magazines
□ Celebrity News (e.g. People)
□ Fashion Magazines (e.g. Elle)
□ Financial News (e.g. Bloomberg Business)
□ Interior Magazines
□ Special topic blogs (e.g. Security, Hobbies etc)
□ Local News

□ Other
□ I don’t read news online
□ I don’t know

Our values form our attitudes and opinions, this is why we ask you about your political views. Our values form our attitudes, opinions and behaviour. For that reason, you are in the following question asked to indicate where you position yourself in the political spectrum.

This question is not mandatory, and we kindly remind you that this survey is anonymous. Thus, please keep in mind that we cannot trace your answers back to you.

9) Which of these political ideologies matches your views?

○ I choose not to answer
○ Democrat
○ Conservative
○ Liberal
○ Labour
○ The “Green” movement
○ Other
○ I am not entitled to vote
○ I don’t know

Technology plays an increasingly important role in our society. On this background, we will in the following section ask you a series of questions that relate to your opinions on online safety.

10) * State your level of agreement on the following statements?

	I fully disagree	I partly disagree	I partly agree	I fully agree	I don’t know
I am positive towards using new technology					
I know what cybersecurity is					
I expose myself to risks when I am on the Internet					

I am well informed about online threats
I accept that my activities online are monitored if it makes me safer online
Law enforcement agencies will assist me if I am subject to cybercrime
One should be able to be anonymous on the Internet
The Internet will not be safer even if my personal computer is secure
I am confident that the government can secure all information concerning me
Cyber activists (eg. Anonymous) play a role in the fight against cybercrime and cyberwar

11) * I sometimes deliberately break cybersecurity regulations

○ Yes
○ No
○ I don’t know

12) Do you see yourself as capable to assess what is safe or unsafe to do online?

○ Yes
○ No
○ I don’t know

13) Do you think it is safer to shop at domestic rather than foreign online stores?

○ Domestic online stores are safer
○ Foreign online stores are safer
○ They are equally safe/unsafe
○ The important thing is whether they are well known and recognised
○ I don’t know

14) Where is cybersecurity most important to consider?

O At home
O At work or at school
O It is equally important both places
O It is not important anywhere
O I don't know

"Cybersecurity" is a term that refers to how we protect the information that is important to us online.
In this section, we will ask you about how you relate to different types of threats.

15) * How worried are you that the following will happen to you? (1: Not worried at all. 5: Significantly worried)

	1	2	3	4	5	I don't know
That my bank- or credit cards will be used in online fraud						
That others will use my identity online						
That I will be bullied or harassed online						
That my digital documents or pictures will be destroyed or deleted						
That a virus will infect my computer						
That I will be manipulated to send sensitive information to someone						

16) * How much risk do you associate with the following activities? (1: Very low risk. 5: Very high risk)

	1	2	3	4	5	I don't know
Using online banking						
Using email						

Sharing passwords with others
Using the same password at several online services
Using bank or credit cards online
Using online gambling
Using social media
Not back-up your data
Using public (government) services online

17) * What is your most likely course of action if the following happens to you?

	I will do nothing	I will take care of it myslef	I will seek help from an expert	I will report it to a law enforcement agency	I don’t know
You are bullied or harassed online					
You are subject to online fraud					
Your home computer is infected with a virus					
Your online identity is stolen					

18) Has information concerning threats and hacking made you refrain from using an online service?

O Yes
O No
O I don’t know

19) What do you think is your largest online threat?

O That you will do something yourself that compromises your online safety.
O That someone else will do something to you (eg. hack a site where you have some personal information)

Interests, knowledge and behaviour often go hand in hand.
In this section, we will ask you about what you are interested in, and how you obtain knowledge about cybersecurity.

20) * How interested are you in information technology? (1: Very little interest. 5: Very interested)

○ 1
○ 2
○ 3
○ 4
○ 5
○ I don't know

21) * Do you know more or less about cybersecurity than the average person?

○ I know more than the average person
○ I know less than the average person
○ I know the same as the average person

22) * From whom do you usually learn about cybersecurity?

○ I teach myself
○ I learn from experts
○ I learn from my managers or teachers
○ I learn from friends, colleagues or classmates
○ I dont know

23) How do you usually learn about cybersecurity?

○ Trial and error by myself
○ Formal education or courses
○ I learn from others in an informal setting
○ I don't know

24) * Have you received formal cybersecurity training within the past two years?

○ Yes
○ No
○ I don't know

25) * Does your workplace or school have rules for cybersecurity?

○ Yes
○ No
○ I don't know

26) * Are you allowed to use your private computer at your workplace or school?

○ Yes
○ No
○ I don't know

27) Do you think that your cybersecurity skills have improved after your cybersecurity training?

○ Yes
○ No
○ I don't know

28) * What kind of cybersecurity software do you have on your home computer? (Multiple answers are possible)

□ Firewall
□ Anti-virus
□ Other cybersecurity software
□ I don't use any cybersecurity software
□ I don't have a computer at home
□ I don't know

29) * Do you assess whether a website is safe before you use it?

○ Yes, always
○ Yes, usually
○ Yes, sometimes
○ No, never
○ I don't know

For this question, we want to know how you use passwords in a private setting, not at work.

30) * How do you use passwords? (Multiple answers are possible)

□ I use the same password everywhere
□ I use a password manager for most of my passwords
□ I use different password for most online services
□ I try to create secure passwords
□ I don't know

For this question, we want to know how you back-up your data in a private setting, not at work.

31) * How often do you back-up data that is important to you?

○ Every week, or more often
○ Every month
○ Less often than every month
○ Never
○ I don't know

32) * If you were to sell or throw away your personal computer, would you first make sure that all personal information is deleted securely?

○ Yes
○ No
○ I don't know

33) * Do you have routines for updating the software on your personal computer?

○ Updates happen automatically
○ I update them manually once the updates are available
○ I have no routines for updating
○ I don't know

34) Do you have any comments concerning this survey?

Teknologiveien 22
2815 Gjøvik
Org.nr: 995 195 003

Telefon: 40 00 58 99
Nett: www.norsis.no
E-post: post@norsis.no

NorSIS