Master's thesis

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

Gard Hoel Grøttan

Security Awareness of Students at NTNU

Master's thesis in Information Security
Supervisor: Gaute Wangen
Co-supervisor: Vasileios Gkioulos
May 2021

NTNU
Norwegian University of Science and Technology

Gard Hoel Grøttan

Security Awareness of Students at NTNU

Master's thesis in Information Security
Supervisor: Gaute Wangen
Co-supervisor: Vasileios Gkioulos
May 2021

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

NTNU

Kunnskap for en bedre verden

Abstract

The purpose of this study is to determine the level of security awareness of students at NTNU, in regards to the university's information security training that is directed at students. This study was conducted using an online questionnaire to gather quantitative data. The questionnaire was distributed on different platforms where the majority of users are students, in addition to contacting students directly through student e-mail. The results of this study suggests that the security awareness of students at NTNU is sufficient, however, that there are multiple points of improvement in various categories. Overall, students associated with a technical faculty tends to score slightly better than compared to students from a non-technical faculty.

Sammendrag

Hensikten med denne studien er å avgjøre til hvilken grad studenter ved NTNU er sikkerhetsbevisste i henhold til universitetets informasjonssikkerhetsopplæring som er rettet mot studenter. Studien ble gjennomført via en nettbasert spørreundersøkelse for å innsamle kvantitative data. Spørreundersøkelsen ble distribuert på ulike platformer hvor flertallet av brukerne er studenter, i tillegg til at studenter ble kontaktet direkte gjennom e-post. Resultatene fra denne studien indikerer at sikkerhetsbevisstheten til studenter er tilstrekkelig, men at det også finnes forbedringspotensiale innad flere kategorier. Alt i alt, viser studenter som er tilknyttet et teknisk fakultet bedre resultater sammenlignet med studenter fra ikke-tekniske fakultet.

Contents

Figures

Tables

Chapter 1

Introduction

Institutions for higher education are targets for both individual and state funded adversaries. In a 2021 report by Bluevoyant [1], a cybersecurity service company, ransomware attacks are the biggest threats to universities, where such events have doubled from 2019 to 2020. The report states that the average cost of a ransomware attack in 2020 was estimated to be $447,000, or roughly 3,7 million NOK. It is further stated that not only have ransomware attacks against universities and educational institutes become more expensive and frequent, but due to the Covid-19 pandemic and the appliance of digital learning tools, the attack surface at universities have expanded. Following ransomware, the report also states that data breaches and data theft by other nations make up for the second and third most prevalent threat, respectively.

In line with the Bluevoyant report, there is no shortage of recent news that reflects the concerns that are raised. The further education newspaper (FE week) reported a major ransomware attack against Birmingham colleges [2], where the institute's servers and workstations were encrypted, and data were extracted from their servers. The BBC reports of three universities in different location targeted at the same time [3], where universities in Lancashire, Scotland, and Belfast experienced an attack on their student learning systems. An FBI industry alert [4] reports an increase in ransomware attacks in US and UK-based universities, and describes in detail what kind of ransomware is used and how it works.

Norwegian universities have also been targeted. A TV2 interview with the department director of the national section for cybersecurity [5], following a cyberattack on the Artic University of Norway (UiT), state that cyberattacks have become more common, and that adversaries, both individuals and state sponsored actors, have become more prepared and launched more complex attacks.

[1] https://www.bluevoyant.com/resources/cybersecurity-in-higher-education/ (Accessed: 18.03.21)

[2] https://feweek.co.uk/2021/03/15/college-group-closes-all-campuses-for-a-week-following-major-cyber-attack/ (Accessed: 18.03.21)

[3] https://www.bbc.com/news/uk-england-lancashire-56347708

[4] https://www.ic3.gov/Media/News/2021/210316.pdf

[5] https://www.tv2.no/a/11841152/

An article published in Nasdaq [6] titled "Why Future-Proofing Higher Education is Simpler Than It Sounds" discusses how educational institutes should move forward in preventing security breaches. They suggest that cybersecurity bootcamps are viable options in order to accommodate for the lack of security employees, and they suggest that governments should take actions to address the shortage of cybersecurity professionals.

1.1 Topics Covered by the project

Topics covered in this project will evaluate the security awareness of students at the Norwegian university of science and technology (NTNU). By security awareness, three individual factors are considered; information security knowledge, attitude towards information security, and information security behaviour. By information security knowledge, it is meant the level of understanding and knowledge an individual has in regards to threats, cybersecurity jargon, and knowledge of preventative actions. Security behaviour encompasses the planned actions of an individual, and should be based on the level of information security knowledge one possesses. In order to assess these factors, this project utilised a survey for identifying the level of security awareness among students at NTNU.

1.2 Keywords

Information Security, Information Security Awareness, Higher Education

1.3 Problem description

Instead of identifying and exploiting a weakness in a technical system, an adversary might choose to target an authorised user of the system instead, where the adversary attempts to persuade the legitimate user to give up confidential information. This type of social manipulation is effective due to the lack of information security awareness from the victim, where they might not be knowledgeable of potential threats, and thus behave in a non-compliant manner that leads to security incidents. Students at NTNU have access to information, research, and infrastructure that might be of value to adversaries, and should therefore be aware of potential threats, both social manipulation and technological exploits, in order to behave in a preventative manner that minimises the risk of security incidents.

[6] https://www.nasdaq.com/articles/why-future-proofing-higher-education-is-simpler-than-it-sounds-2021-03-17

1.4 Justification, motivation and benefits

Identifying and assessing the level of security awareness of students at NTNU might aid in further developing awareness programs and the information security training of students. Discovering gaps and strengths in security awareness of students might be crucial in reaching the security objectives identified in the university's information security policy [7], where among other objectives, it is stated: "All employees, students, and others who have access to, and/or process and manage information through NTNU's ICT infrastructure, must be familiar with and comply with NTNU's requirements for information security".

Additionally, among the research that has been conducted in regards to security awareness at NTNU, only employees have been the target groups. With the amount of students outweighing the number of staff, social manipulation against students is a noteworthy threat against the university's infrastructure and information.

1.5 Research questions

Based on the problem description, the following research questions have been identified:

1. How knowledgeable are students at NTNU with information security concepts related to the university's policies and guidelines?
2. What are student's attitude towards information security concepts related to the university's policies and guidelines?
3. How does student's security behaviour compare with the expected behaviour related to the university's policies and guidelines?

1.6 Planned contributions

This thesis contributes to the gathering of data that aims to identify the level of security knowledge, security attitude, as well as identifying the security behaviour of students, in regards to the university's training and courses. Additionally, this study aims to present, analyse, and discuss the overall level of security awareness among students at NTNU.

1.7 Structure of the thesis

The thesis in total consists of seven main parts, and can be summarised as the following:

[7] https://innsida.ntnu.no/wiki/-/wiki/English/Policy+for+information+securitysection-Policy+for+information+security-About+Policy+for+information+security

Chapter 2 Defines security awareness in the context of this thesis, and gives a brief background on security awareness in higher education, as well as security awareness at NTNU.

Chapter 3 Aims to present the existing literature in regards to the above stated research questions, and identify what has already been established.

Chapter 4 Presents the applied methodology that is used for the data collection for this project.

Chapter 5 Presents the results of the questionnaire.

Chapter 6 Discusses and attempts to highlight the major findings of this study

Chapter 7 Aims to give a satisfactory conclusion in regards to the overall result and discussion.

Chapter 8 Presents and discusses limitations and future work.

Chapter 2

Background

This chapter aims to accomplish three main goals: (1) Give a reasonable definition of security awareness in the context of this thesis; (2) Present a brief overview of the need of security awareness and its importance; (3) Present a brief overview of the implications that security awareness has in the context of educational institutes.

2.1 Defining security awareness

Before presenting the importance and the impact that security awareness has in educational institutions, the term needs to be defined in order to communicate its implications and boundaries in the context of this paper. This section will attempt to define the term based on previous work that have similar approaches.

Norman Hänsch et al. [1] conducted a literature review on how "IT security awareness" is used in previous studies. Their findings suggest that there is no common agreement on the definition of security awareness, and that developing a common understanding of the term might not be feasible, due to the varying scopes in which the term is applied. The authors further present an overview of the measurement methods used in previous literature:

- Feedback towards experts
- Self assessment
- Knowledge test
- Observation of users

Developing a universal definition of the term is beyond the scope of this paper, and thus, the definition of security awareness will be used in accordance with definitions applied in studies with similar methodology, which in this case are definitions applied in the context of measuring security awareness through self assessment.

As of a result of the approach and methodology of this work, the definition of security awareness is adopted from Parsons et al. [2], where the authors define the term as: "ISA should consider both the extent to which an organisation's em-

ployees understand the importance and implications of information security, and the extent to which they behave in accordance with the organisation's information security policies and procedures". This definition is based on the "Knowledge-Attitude-Behaviour" (KAB) model, and the authors argue that an individual's increased knowledge of security behaviour increases their attitude, which then improves their security behaviour.

Thus, in the context of this work, security awareness will refer to the collection of an individual's knowledge, attitude, and behaviour of information security, in line with rules and regulations given in policies and guidelines.

2.2 Why measure security awareness?

According to Lebek et al. [3], organisations have in the past years become highly dependent on being able to handle and process information, and in order to protect themselves from threats to their information security, technical measures are implemented in order to mitigate these threats. However, these technical implementations are only effective as long as the end-users of the information systems are aware of the potential security threats.

Aloul [4] also suggests that the use of advanced technological security solutions, and the employment of security professionals has diverted the focus on end-users, where effort is missing in educating the "normal" users of the systems, thus, leaving them as the weakest link. The author further suggest that this results in adversaries targeting the uneducated users, as they make for easy targets due to the raised technical security.

These factors are also pointed out in a paper by Dr. John Leach [5], where he argues that the level of thoroughness in policies and documentations cannot account for all the varying situations that an employee might encounter, which means that an organisation has to rely on their employees to make rational choices for security during their daily operations. Additionally, a paper by David Lacey [6] also presents that even though security incidents are caused by non-compliant behaviour of end-users, their actions are also the reason incidents are detected and prevented. The author further presents that in most cases, incidents are not caused as a result of intentional non-compliant behaviour, but rather from factors such as lack of training, stress, or bad system or process design.

It is clear from the aforementioned literature that in order to fully protect an organisation's information systems, not only should the technical aspects be considered, but there should also be a heavy emphasis on the end-users of the systems. According to Legard's "Building an effective information security awareness program" [7], in order to achieve protection against threats that end-users face, such as social manipulation, security awareness programs can be an effective tool. The author further presents that the most successful security awareness programs are those that the users feel are relevant and applicable to themselves, and that the programs which reflects the current security awareness of its users. To the same degree as business-oriented organisations, it is also suggested that educational

institutes should offer its students (end-users) dynamic awareness training in line with both emerging and disappearing security threats [8].

2.3 Why higher education institutes?

In line with the concerns that are raised for traditional businesses, Rezgui et al. [9] states that the case of information system security managers focuses their attention towards technical security solutions, while spending less time on threats created by lack of awareness from end-users. The authors further explain that this is highly problematic in higher education institutes, due to the nature of these institutions being public and having considerable amounts of computing power and information flow. Furthermore, the authors also express concerns in regards to the lack of training of both staff and students, and suggests that universities are among the least secured environments.

In an investigative study, conducted by Hina et al. [10], the same concerns for imbalanced focus between technical and human aspects of security are raised, and it is argued that the lowered awareness leads to non-compliant behaviour. Another study conducted by Hina et al.[11], the authors review the current literature in regards to compliance of security policies in higher education institutes, and state that these institutes face the same threats as traditional businesses. Furthermore, it is stated that, unlike business-oriented organisations, higher education institutes fail to realise the degree of their information sensitivity, and thus fail to properly raise awareness of its users.

Further expanding on the statement of awareness training of students, as previously described by [8], it is suggested that the training should be carefully planned and managed in order not to cause the opposite intentional effect; if the given awareness training is not sufficient enough, an individual might develop a false sense of security, and thus act recklessly, believing they have the correct knowledge to protect themselves.

In terms of specific vulnerabilities, Ulven and Wangen [12] conducted a comprehensive literature review on the biggest cybersecurity threats in higher education institutes, and presents a categorical overview of the most valuable assets, the most prominent threats, in addition to its associated consequences. From their analysis, the following categories are listed as the most valuable assets in higher education:

- Personally identifiable information on students and staff
- Financial data
- Research data
- IP
- Student grades
- Administration details

The security events that targets these assets are identified as intrusion, malware, asset scanning, social engineering, and unintentional disclosure. From the

presented assets and the associated threats, the authors presents the following categories as the potential consequences for successful attacks on the above-mentioned assets:

- Data leakage
- Data loss
- Financial fraud
- Loss of availability
- Abuse and attack on data integrity

To summarise the need for security awareness in higher educational institutes, educational institutes faces much the same troubles as traditional businesses, however, these institutions are more publicly facing with vast amounts of information. Additionally, educational institutes have been shown to be prone to the same threats and risks that traditional companies face. The need for security awareness is further strengthened by the transient nature of students, and there is a need for continual assessment of both the threat landscape, and the training of students and staff.

Chapter 3

Related Work

The purpose of this chapter is to present what has previously been researched on the topic of this thesis. The research questions presented in the introduction are closely related, and have for the majority of previous research been studied as a combination. For this reason, it would not be feasible to present each research question individually, but rather present the related work as a whole. This chapter will present the related work for the following topics: (1) Security awareness of students in higher education institutes, and (2) Security awareness at NTNU. Lastly, the aim of this chapter is also to uncover any gaps in the current literature that does not feasibly answer the presented research questions.

3.1 Measuring security awareness

In 2006, Kruger et al. [13] developed a prototype for assessing the level of security awareness. The aim of the study was to assess the security awareness of employees in a gold mining company. In their prototype, a questionnaire was developed based on identified focus areas of information security, such that the questionnaire was applicable towards the specific target group. Furthermore, the questions were designed with the intention on measuring the knowledge, attitude, and behaviour of the respondent, where each question was to be answered on either a three-point scale (true, false, I don't know), or a two-point scale (true, false). Limitations for this approach is expressed by the authors, where self-reported behaviour from respondents should not be considered an accurate reflection of actual behaviour, but it should rather be an indication of the security behaviour displayed by the respondents.

Parsons et al. [14] employed a similar approach, where the main objectives of the study was to determine the knowledge, attitude, and behaviour of Australian government employees. Unlike the approach from Kruger et al., the questions were created based on aspects of InfoSec management, were the aim was to identify the general computer practice of employees. A three-point scale (true, false, don't know) was used for identifying knowledge, while a five-point scale

was applied to measure attitude and behaviour. Furthermore, the authors recognise the limitations of self-reported questions, and in order to attempt to mitigate response bias, negatively worded questions were implemented.

Later, Parsons et al. [15] began a study in which the aim was to develop a questionnaire for assessing the human aspects of information security (named HAIS-Q), in addition to assessing the relationship between the knowledge and attitude towards policies and procedures, and the corresponding behavior. When developing the questionnaire, the authors approached the problem in the same manner as Kruger et al., where they considered the existing policies and procedures that are relevant for the respondents. Based on these relevant areas, sub-categories were identified in order to determine common human errors, and for each sub-category, a question related to knowledge, attitude, and behaviour was created. In contrast with the research of Kruger et al. [13] and their previously presented work [14], each question is measured on a five-point scale instead of combining varying number of scales. The results of their study indicates that there is a positive relationship between the knowledge and attitudes of policies and procedures, and the behavior of respondents. Parsons et al. [2] also conducted a further study on the use of the HAIS-Q questionnaire, where the questionnaire was proven to be an effective instrument for measuring security awareness of both students and government employees.

3.2 Security awareness of students in higher education institutes

Eyong [16] conducted a study in which undergraduate students in a business college were surveyed, in order to determine their understanding and attitudes towards information security. The author developed a questionnaire based on previous works and the NIST 800-50 guideline for building a security awareness and training program. The results of the study indicate that students were well aware of the many topics and concepts in information security, however, gaps were also uncovered in regards to knowledge about phishing. Their results also show that even though the students understand the need for training, many did not realise that the university offered training on information security. The author concludes that security training should be mandatory for first-year students, and that the training programs should reflect the current awareness of students in order to cover the missing gaps in their knowledge. The author argues that a generic approach to training might not be as effective, and might be less attractive to students.

Filippidis et al. [17] presents a study with the purpose of determining the security awareness and computer ethics of computer science students in a Greek university. They applied a questionnaire due to the ease of distribution and it's ability to compare with similar studies. The authors noted, however, that such a questionnaire lacks validity. The results of the study indicate that students are

aware of the concepts in information security, however, there is a lack of knowledge and appropriate actions. Their findings also indicate that the level in which students are studying at has an impact on their awareness, where students at a master's level exhibited better awareness compared to the students at a bachelor's level. The study discusses it limits where only non-IT students are considered, and where only a single university is considered.

Supporting the findings of Filippidis et al., Törley [18] considered only first-year students in his research. The author developed a questionnaire on simple information security awareness statements, which included both theoretical and practical questions. The aim of the study was to uncover gaps in the knowledge of students from high school, as well as the security awareness of first-year students. Their results indicate that most of the students believe they are aware of security, however, the majority of respondents show uncertainty on even basic concepts of information security awareness. The overall results displays that first-year students have a low security awareness, and that even though students have experience with security awareness, there is a lack of knowledge. Similar findings were also discovered by firmansyah et al. [19]. The aim of their study was to determine the security awareness of students that were in their third year, and was affiliated with the university's department of information systems. The authors created a questionnaire based on the KAD-model, where an individual's knowledge, attitude, and behaviour was considered. Their results show that the students have a moderate level of security awareness, where it was discovered that students were lacking knowledge on the classification of university resources, their attitude towards dealing with sensitive information was insufficient, and their behaviour regarding password sharing was considered low.

Somewhat contrary to the aforementioned studies, Kiss [20] questioned kindergarten teacher students at the beginning and students at the end of their studies. The author utilised a questionnaire asking about ICT equipment, their internet habits, and their password usage. The results show that students at the beginning of their study have low awareness, however, students that are at the end of their studies did not show any increase in awareness, and they conclude that by simply attending higher education, one's security awareness does not increase.

Not only does the literature raise concerns regarding the awareness of students in universities, but Garrison et al. [21] also discusses the effects this can have when students are graduating. In their particular research, they raise concerns regarding accountant students, where work in this field involves access to personal sensitive information of clients. In their work, the authors assesses the security awareness of accountant students, and discover that students may not be feasibly prepared for handling sensitive data. Additionally, their results indicate that the biggest gap in knowledge and behaviour is in regards to using anti-virus and being aware of malicious e-mails.

3.3 Security awareness at NTNU

Work conducted on the particular subject of assessing the security awareness at NTNU is by no means exhausted, however, there are a couple of studies that have conducted work in assessing the cybersecurity at the institution. Most notably, "Mørketallsundersøkelsen 2018" by the NTNU IT department [22], aimed to investigate non-reported security incidents at NTNU, where target respondents were employees at the university. Among others, the most notable reported findings include incidents related to knowledge of reporting, misuse of university ICT-equipment, phishing/social engineering, industry espionage, leakage of personal information, and insecure storing of research data.

From the survey, it is reported that below half of respondents were knowledgeable of how to report incidents and/or security discrepancies. Even though a small percentage of respondents reported that they knew of co-workers using university ICT-equipment to mine cryptocurrency, however, no such incidents have been reported or discovered by the Security Operations Center (SOC) at NTNU. Furthermore, almost half of employees reported to have experienced social engineering, and the number of employees who knew of co-workers that had fallen victim to such types of attacks exceeded the number of known attacks with negative consequences, meaning that there is a reasonable probability of unknown negative consequences related to phishing/social engineering attacks. There were few reports of experiencing or believing in the occurrence of industry espionage, however, despite the low reported incidents, these types of incidents can be severe. Lastly, in regards to leakage of personal information and storing of research data, few employees knew of incidents where personal data was leaked; among those who reported that they knew of incidents, almost all of them are technical administrators, which is suggested to imply a high number of unreported incidents. Above half of the respondents reported that sensitive research data is being stored in a non-secure manner to some degree or more often, however, only a small number of employees report that they know of incidents where confidential information has been leaked. The report concludes that it is the first of its kind to uncover that there are occurrences of industrial espionage and illegal extraction of information at NTNU. The authors also suggest that employees at the university has a big potential for improvement in reporting security incidents and discrepancies, and that NTNU itself has show to have insufficient practices in regards to both physical and logical securing of information.

Another study conducted on the security of NTNU, is a Bachelor's thesis that aimed to investigate the security culture of IT-employees at the university [23]. Among other goals, one of the sub-goals of this thesis was to determine the security culture of IT-employees through a survey. The authors investigated a series of dimensions related to security culture, and utilised their results to create an action plan. The results from their survey suggests that the IT-departments have points for improvement in regards to training, management anchoring, department structure, and information governance. On the other hand, the following

points were presented as strong points; Management, risk assessment, incident handling, and ethical conduct.

In summary, the IT-department seem, for the most part, to have an acceptable security culture. Comparing the results from "Mørketallsundersøkelsen", the employees that are employed within technical administration are also shown to have greater knowledge and awareness of information security. From these studies, it has been shown that technical staff has better knowledge and culture in regards to information security and information technology, however, both of these studies are concerned with the employees at the university, and not it's students. From the presented results in these works, it might be fair to assume that there exist a similar dynamic among students, both technical and non-technical.

Chapter 4

Methodology

4.1 Choice of method

The purpose of this thesis is to determine the level of security awareness of students at NTNU. As presented in the related work, there are many methods and possibilities to consider for measuring security awareness. A qualitative approach could be applicable, however, due to the time constraints of the thesis, and the requirement for both a representative and large enough sample of students, it would require too much time. Another option could be to implement some kind of practical test, such as performed by Azmin et al. [24], where the authors performed a penetration test on a campus to determine how a data leak might occur in an educational setting. Although this kind of approach might be very prominent for assessing the actual security behaviour of students, due to the campus restrictions during the Covid-19 pandemic, this approach would not be feasible for this project. From the presented related work, there is a strong preference for using online questionnaire and a quantitative approach. It is likely that this approach is favorable due to the large number of potential participants, and it is also stated by authors that utilising a quantitative approach with an online survey is easier to distribute and compare with other studies [17]. A quantitative approach might also be the best option in regards to answering the presented research questions:

RQ1: How knowledgeable are students at NTNU with information security concepts related to the university's policies and guidelines?

A quantitative approach to answering this question is feasible, as knowledge can be measured with numbers. We are aware of what is considered right and wrong in relation to what is expected of the students to know. The level of knowledge can be measured on a scale, such as a five-point likert scale, or on a simpler (yes/no/don't know) two-point scale.

RQ2: What are student's attitude towards information security concepts related to the university's policies and guidelines?

In the same manner as knowledge, a participant's attitude can also be assessed through numeric evaluation. There are clear guidelines for what constitutes as good and bad attitude towards security, however, there might be different levels of attitudes, and the use of a five-point Likert scale can be more favorable in this case.

RQ3: How does student's security behaviour compare with the expected behaviour related to the university's policies and guidelines?

A quantitative approach to assessing the behaviour of individuals might not be the most optimal approach, and might be skewed due to bias in responses. However, the behavioural element is measured along with knowledge and attitude, and could aid in identifying the general behaviour rather than each individual's actual behaviour [13].

4.2 Data collection

In order to collect data for this project, a questionnaire with closed-ended questions in a likert-scale fashion was utilised to collect quantitative data. This means that for each question in the survey, the answers are pre-defined on a scale, which in this case ranged from 1-5. The distribution of the questionnaire was deployed through various means; the survey was posted on an internal digital bulletin board at "Innsida", a sub-reddit for NTNU students, and sent directly to students through student e-mail. A copy of the questionnaire was created for each aforementioned platform in order to keep control of the number of answers for each method of distribution. The reason for choosing these distribution channels is due to the target population being students. In all cases where the survey was distributed, an English and Norwegian variant was included to account for exchange students.

4.2.1 Bulletin board

The bulletin board at "Innsida" is an internal page for students and employees at the university, and individual's who aren't enrolled or employed by the university cannot access this page without university credentials. This means that it is difficult to control whether any employees or staff partakes in the survey, however, additional measures for this has been implemented in the questionnaire.

4.2.2 Social media

The sub-reddit for NTNU students, however, is a public forum where there is no need for proving that you are a student or an employee at the university. This

might create the risk of gathering data from individuals outside of the target population, however, due to the large number of students, it might be feasible in order to gather enough samples.

4.2.3 E-mail

E-mails were sent out through an internal e-mail service, where recipients can only be individuals that are in some way associated with the university. By sorting recipients by their roles and faculties, e-mails were deployed to people who had the role of "student", and were associated with a certain faulty.

4.3 Questionnaire design

The baseline for the survey is based on the HAIS-Q questionnaire, developed by Parsons et al. [15]. The HAIS-Q questionnaire is a module-based survey for measuring knowledge, attitude, and behaviour, which means that the survey itself is created by combining modules that are concerned with different aspects related to information security. The modules themselves are based on common human errors that are identified through information security policies. By utilising modules, it can allow for a customised design than compared to what Parsons et al. conducted, but at the same time keep the validity of the developed questionnaire. It order to fully utilise this method, it might be beneficial to revise the HAIS-Q modules in accordance with the security policies that NTNU has identified to be relevant for its students. In order to identify the needed modules, the training and courses directed at students were used. Table 4.1 displays the identified modules and their respective categories in regards to the security policies that NTNU provides to its students.

Table 4.1: Identified modules and their categories

Module	**Categories**
Password management	- Strong password - Unique password
Internet use	- Internet presence - Downloading files
E-mail use	- Sending confidential/sensitive information - Receiving confidential/sensitive information - Clicking links
Reporting of incidents/discrepancies	- The importance of reporting - What should be reported
Computer security	- Updated operative system and applications - Anti-virus - VPN
Mobile devices	- Strong passcode - Remote wipe
Information handling	- Be careful of what information you share

The next step is to compare the modules that were identified with the modules from the HAIS-Q method. Modules that match will be kept, while non-identified modules from the HAIS-Q will be omitted, and newly identified modules from the NTNU policies will be added. Table 4.2 displays the HAIS-Q modules compared with identified modules from the student information security training at NTNU.

Table 4.2: Comparison of HAIS-Q and identified modules

HAIS-Q modules	**Identified modules**
Password management	Password management
Internet use	Internet use
E-mail use	E-mail use
Incident reporting	Incident reporting
Social media use	Computer security
Mobile devices	Mobile devices
Information handling	Information handling

From the above presented table, we can observe that the modules are the same for the most part, which is expected, as the HAIS-Q is already based on common human errors. However, as highlighted in the table, "Social media use" has been omitted in favour of "Computer security", as this better reflect the training that NTNU provides.

The HAIS-Q method was also utilised in creating the questions for the survey. For each module, each of the KAB dimensions are implemented (knowledge, attitude, behaviour), and each of these dimensions contain three questions each. This means that the total number of module-related questions are: 7 (number of modules) × 3 (number of dimensions) × 3 (number of questions for each dimension) = 63 questions in total (excluding demographic-related questions and optional feedback-field).

The questions were created based on questions given in the HAIS-Q, however, small modifications have been done in order to better reflect the environment and policies that are present in this study. In the adopted methodology, the questions are phrased in a way that targets employees of an organisation, while for this particular study, the questions needs to be phrased such that they are applicable towards students. For example, in the knowledge dimension regarding password management, the HAIS-Q questionnaire has the following question: "I am allowed to share my work passwords with colleagues". In the modified version, this question has been changed to "I am allowed to share my school account passwords with classmates". Such changes has been done for all questions that did not apply to the targeted environment and population. The full questionnaire can be found in Appendix A.

4.4 Ethical and legal considerations

The collected data for this project was performed in such a manner that all answers were anonymous, and there would be no possibility to link any information to a specific individual. The respondents did, however, have the option to submit their e-mail in order to be able to win a gift card for completing the survey. If the respondents wished to submit their e-mail, it was done through a separate form in order to not link any of their answers to their e-email. Additionally, the questionnaire was approved by the Norwegian Center for Research Data (NSD). After the collection period ended, a random e-mail was drawn using an online tool, and the collected e-mails were deleted. The anonymity of the data and the transparency of this project was fully described in the questionnaire to make sure that the participants were aware of how the data was being handled.

Chapter 5

Results

This chapter aims to present the data that was collected through the methodology described in the previous chapter. This chapter will be divided into sub-sections according to each respective section in the questionnaire. Furthermore, the results will be presented with a textual description, followed by a visual representation where it is feasible.

5.1 Population and sampling

After the data collection period ended, the survey had a total of 111 respondents. Of the 111 responses, 8 respondents reported that they were employees. Since we are only interested in students, these answers were omitted. Additionally, 11 respondents did not complete the questionnaire, and their answers were also omitted. In total, the questionnaire received 92 valid responses. From the distribution channels, 48 respondents were obtained from e-mail recruitment, 8 responses were gathered from Reddit, and 55 were obtained from the bulletin board at Innsida. It is difficult to determine the response rate for Reddit and Innsida, as we do not know the number of students who knew of the survey. For e-mail responses, a total of 850 e-mails were sent from mid-April to early-May, meaning that the response rate for e-mail recruitment was roughly $48/850 = 5\%$, which is quite low. Furthermore, from the obtained results, students were also grouped into either "technical students" or "non-technical" students. This grouping was based on the nature of the faculties, where the faculty of Information Technology and Electrical Engineering (IE) and the Faculty of Engineering (IV) makes up the "technical students", and the remaining six faculties makes up the "non-technical students" group. In total, the "technical students"-group had $N = 47$ usable responses, and the "non-technical students"-group had $N = 45$ usable responses.

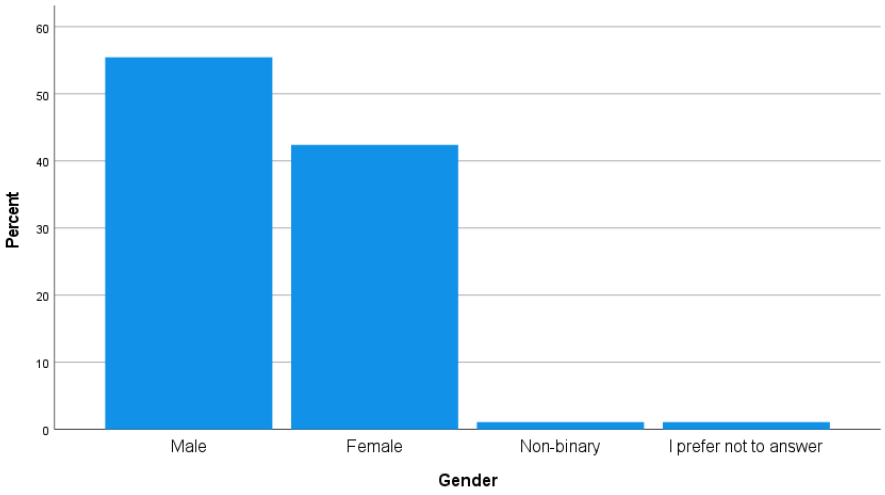


Figure 5.1: Gender distribution

5.2 Demographics

This section aims to present the demographic data that was gathered from (N=92) respondents. The factors of gender, age, and faculty affiliation was included in the survey.

5.2.1 Gender

The gender distribution of respondents shows a majority of males, where 55,4% of respondents reported as male, 42,4% reported as female, and the remaining responses were distributed evenly between "non-binary" and "I prefer not to answer".

5.2.2 Age

Considering the target population consists of students, it is expected that the age distribution leans towards a younger age group. 84,8% of respondents were between the age of 20-29, 9,8% reported to be between 30-39, 3,3% reported to be younger that 20, 1 respondent preferred not to answer, and 1 respondent reported to be between 40-49. Figure 5.2 shows the age distribution.

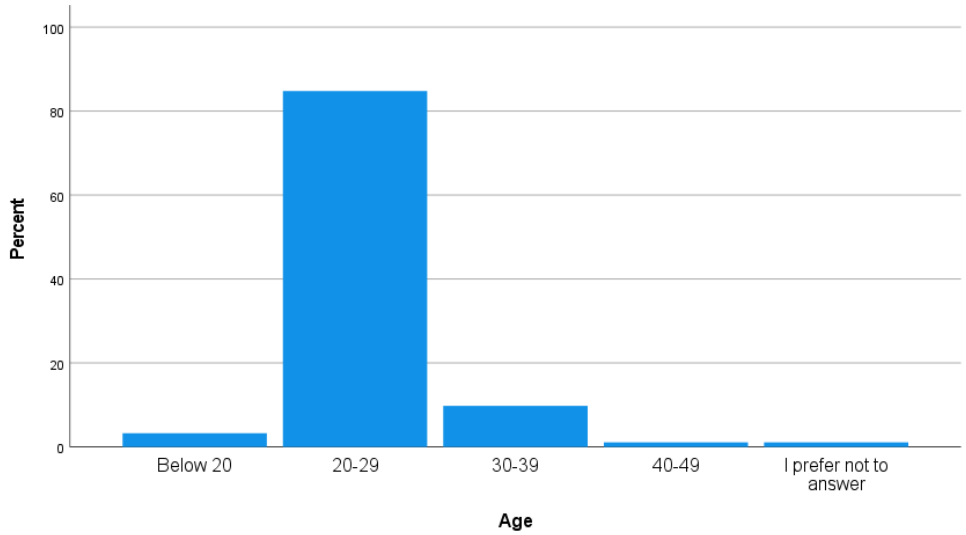


Figure 5.2: Age distribution

5.2.3 Faculty

From the reported faculty affiliation, 38% of respondents affiliate with the Faculty of Information Technology and Electrical Engineering (IE), 14,1% from the Faculty of Natural Sciences (NV), 13% from both the Faculty of Engineering (IV) and the Faculty of Humanities (HF), 7,6% from the Faculty of Architecture and Design (AD), 6,5% from the Faculty of Medicine and Health Sciences (MH), 4,3% from the Faculty of Social and Educational Sciences (SU), and 3,3% from the Faculty of Economics and Management (ØK).

The reason for the outnumbering responses from students affiliated with IE is unknown, however, it can be speculated that this particular subject touches on an area of interest with technical students, and thus, these types of students might be more inclined to answer. Figure 5.3 shows the faculty affiliation distribution.

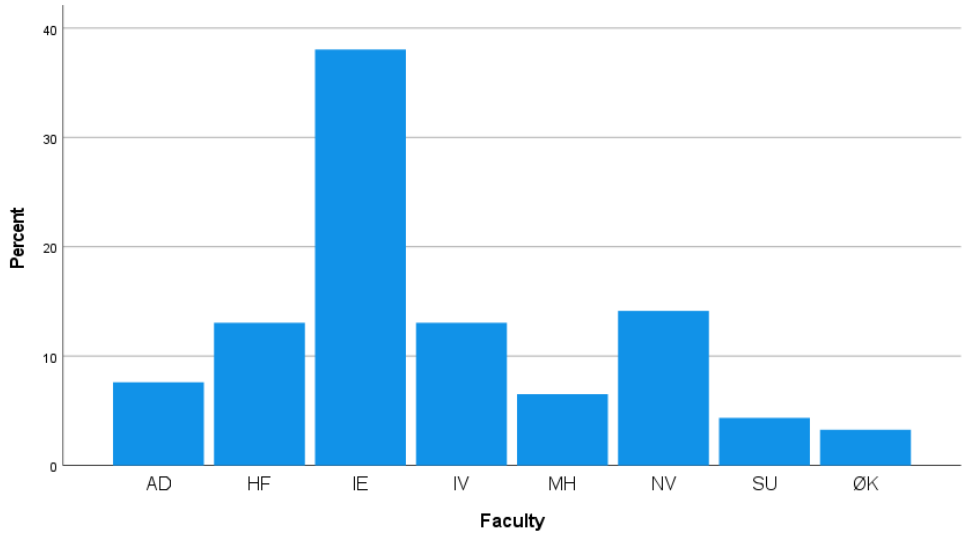


Figure 5.3: Faculty distribution

5.3 General information

This section aims to gather general information about respondents, such as whether they known how to report security incidents/discrepancies, whether they have taken the information security training course, and whether they were aware of such a training course was available to students.

5.3.1 Reporting of security incidents and security discrepancies

Participants were asked whether they know how to report security incidents, and whether they know how to report security discrepancies at NTNU. When comparing the answers between these questions, the "Yes/No" ratio is distributed equally, meaning that the result for both of these questions are the same. In total, 17,4% of students indicated that they know how to report a security incident/security discrepancy, while 82,6& indicated that they do not know how to either report a security incident or discrepancy. The results for both questions are displayed in figure 5.4

5.3.2 Information security course and training

Participants were asked whether they knew that NTNU provides a information security course for its students, and whether they have completed the course. Looking at the first question, 9,8% reported that they knew of the existence of the course, while the remaining 90,2% answered that they were not aware of the existence of the security course. Figure 5.5 shows that ratio between respondents that knew of the provided course.

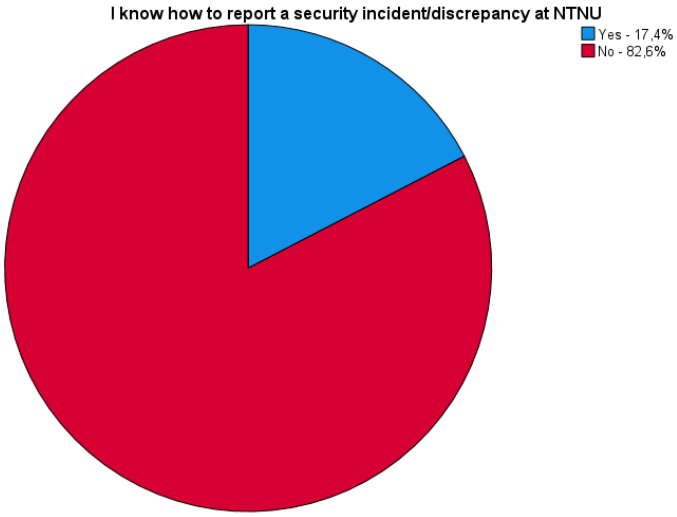


Figure 5.4: Knowledge of how to report incidents and discrepancies

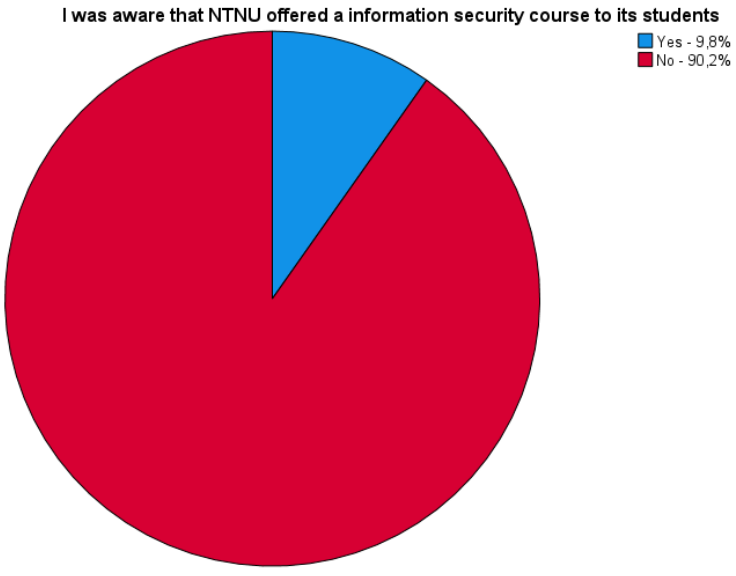


Figure 5.5: Knowledge of NTNU's security course

Similar results were also reported on the subsequent question, asking whether the respondent has completed the course or not. Comparing with the aforementioned result, fewer respondents reported to have completed the course. 3,3% reported to have completed the course, while the remaining 96,7% had not. Figure 5.6 displays the ratio between respondents that have completed the security course.

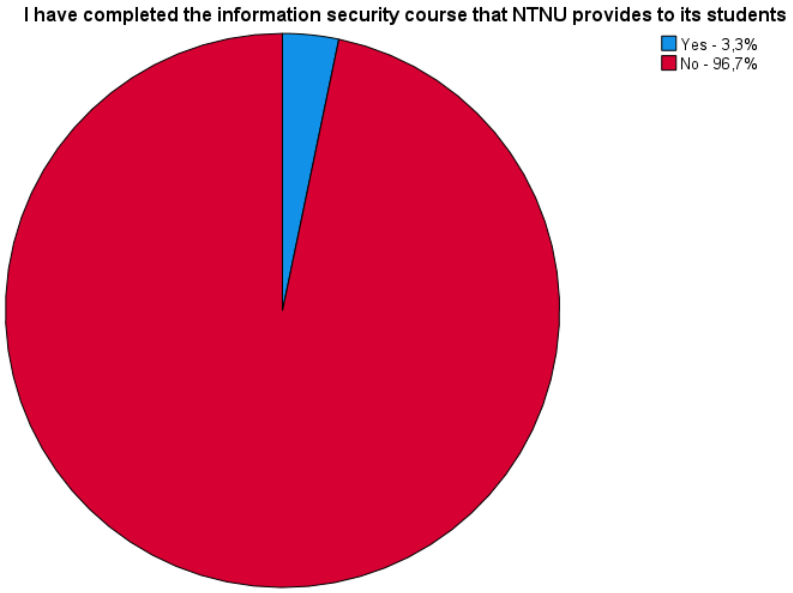


Figure 5.6: Has completed NTNU's security course

5.4 Knowledge, Attitude, and Behaviour

This section aims to present the results of the reported knowledge, attitude, and behaviour in regards to each identified module, as described in chapter 4. In order to present the results in a logical manner, the knowledge, attitude, and behaviour will be presented for one particular module before the results of the next is presented. This way, a module only needs to be presented once. Furthermore, participants were asked to score their agreement on statements regarding each respective topic, on a scale from 1 to 5, where a higher score indicates stronger awareness.

5.4.1 Password management

The module for password management is concerned with re-using passwords, sharing of passwords, and creating passwords. From figure 5.7, we can observe that the mean value across all password management inquiries are generally high, meaning that participants displays an acceptable level of security awareness. We

can observe that respondents are most aware of the dangers of sharing their password, however, we can also observe that there is some difference in answers regarding creating passwords. When asked whether it is necessary to use a mixture of letters, numbers, and special characters in creating a password, the mean value (4,04) is lower compared to when asked whether they use a mixture of these elements when they create passwords (4,4). This indicates that respondents use a mixture of letters, numbers, and special characters, even though fewer report that they know it is necessary.Comparing the means between technical (N=47) and non-technical (n=45) students, there is little difference between these groups, and an Independent Samples t-Test also indicates that there are no significant value, as all of the significance values for each question is above 0,05, and we can thus not assume that there is a difference.

Summarising the results of this first module, the respondents displays a high level of security awareness in regards to password management, regardless if they have a technical background or not.

Descriptive Statistics of Password Management[a]

	N	Range	Minimum	Maximum	Mean	Std. Deviation
It is acceptable to use my social media passwords on my school accounts*	92	3.00	2.00	5.00	4.2500	.95647
I am allowed to share my school account passwords with classmates*	92	4.00	1.00	5.00	4.6413	.70448
A mixture of letters, numbers, and special characters is necessary for passwords on my school accounts*	92	4.00	1.00	5.00	4.0435	1.12819
It is safe to use the same password for social media and school accounts**	92	3.00	2.00	5.00	4.2609	.84995
It is a bad idea to share my school passwords, even if a classmate asks for it**	92	3.00	2.00	5.00	4.6087	.66227
It is safe to have a school password with just letters**	92	4.00	1.00	5.00	3.7065	1.15348
I use a different password for my social media and school accounts***	92	4.00	1.00	5.00	4.3261	.93889
I share my school password with classmates***	92	4.00	1.00	5.00	4.7283	.59491
I use a combination of letters, numbers and symbols in my school passwords***	92	3.00	2.00	5.00	4.4891	.74855
Valid N (listwise)	92					

a. *Knowledge, **Attitude, ***Behaviour

Figure 5.7: Descriptive statistics of password management

5.4.2 E-mail use

The module for e-mail use asks participants about clicking links, and sending and receiving sensitive/confidential information in e-mails. Regarding knowledge of e-mail use, the majority of respondents (46,7%) "Strongly agree" that one should be careful in clicking any links that they receive in their school e-mail. When asked if one is allowed to sent sensitive or confidential information without encrypting it first, the majority (44,6%) answered that they "Strongly disagree" with this statement. When asked whether one should delete sensitive content before forwarding or replying to an e-mail, most respondents (37%) "Agree", however, 32,6% answered that they are undecided. The attitude of respondents scores generally high, where 51,1% indicate that they "Strongly disagree" that links are always safe to click in e-mails, even if they receive the e-mail on their school account, and 41,3% answered that they "Disagree" with this statement. Most respondents "Agree" (45,7%) that sensitive or confidential content should encrypted before being sent in an e-mail, and 40,2% "Strongly agree" with this statement, which is slightly lower than compared to the knowledge dimension. Most respondents also "Disagree" (39,1%) that nothing bad can happen if one does not delete sensitive or confidential content before replying or forwarding an e-mail. For the behaviour dimension, respondents score a slightly lower score. 47,8% "Agree" that they do not always click links, even if they know the sender, 31,5% "Agree" that they do not send sensitive or confidential information without encrypting, however, there was also a close split on "Strongly disagree" (27,2%) and "Neither agree nor disagree" (26,1%). Regarding deleting sensitive content before replying or forwarding an e-mail, the majority is undecided (29,3%), with a close split between "Agree"(26,1%) and "Strongly agree" (25%).

To summarise the overall results, respondents score closely between knowledge and attitude, however, a lower score is indicated for their behaviour. Looking at the difference between technical and non-technical students, figure 5.8 shows the groups statistics between these groups. We can observe that the mean value between the groups are very similar, however, technical students have an overall higher mean compared to non-technical students. Using an Independent Samples t-Test, the questions "It is always safe to click on links in e-mails I receive on my school e-mail" and "It is risky to send sensitive personal or confidential information in e-mails without encrypting the contents first" scores $< .05$ - meaning that the Levene's test is significant, and we cannot assume equal variance between these groups. However, the p-values for these questions are $> .05$, meaning that we cannot assume that there is a significant difference between technical and non-technical students for e-mail use.

It is risky to send sensitive personal or confidential information in e-mails without encrypting the contents first**	Technical students	47	4.1915	.68010	.09920
	Non-technical students	45	4.2222	.95081	.14174
If I receive an e-mail with personal sensitive data or confidential information, nothing bad can happen if I don't delete the sensitive contents before responding or forwarding the e-mail**	Technical students	47	3.9574	.83295	.12150
	Non-technical students	45	4.0000	.82572	.12309
I do not always click on links in e-mails just because they come from someone I know***	Technical students	47	4.0638	.81838	.11937
	Non-technical students	45	3.8222	.98371	.14664
I do not send sensitive personal data or confidential information in e-mail without encrypting the contents first***	Technical students	47	3.8298	1.00691	.14687
	Non-technical students	45	3.5556	1.09867	.16378
If I receive an e-mail with personal sensitive data or confidential information, I delete the sensitive contents before responding or forwarding the e-mail***	Technical students	47	3.6383	1.03052	.15032
	Non-technical students	45	3.4000	1.26850	.18910

a. *Knowldege, **Attitude, ***Behaviour

Figure 5.8: Group statistics for e-mail use

Group Statistics for e-mail use[a]

	faculty_group	N	Mean	Std. Deviation	Std. Error Mean
I should be careful to click on any links in e-mails I receive on my school e-mail*	Technical students	47	4.2128	.80585	.11755
	Non-technical students	45	4.3333	.82572	.12309
I am allowed to send sensitive personal data or confidential information in e-mails without encrypting the contents first*	Technical students	47	4.0638	.94188	.13739
	Non-technical students	45	4.1556	1.02149	.15227
If I receive an e-mail with personal sensitive data or confidential information, I should delete the sensitive contents before responding or forwarding the e-mail*	Technical students	47	3.8298	.89246	.13018
	Non-technical students	45	3.7111	.94441	.14079
It is always safe to click on links in e-mails i receive on my school e-mail**	Technical students	47	4.4468	.54408	.07936
	Non-technical students	45	4.3111	.99595	.14847

5.4.3 Internet use

The section for internet use is concerned with downloading files onto the school computer, and accessing and entering information on websites. In the knowledge dimension, respondent were asked if they think one should be careful in downloading files onto their school computer, and most respondents (59,8%) "Agree" with this statement. Most students also "Agree" that they should not access certain

websites while being at school (40,2%), and that they should be careful in entering information on websites, even if it helps them in doing their schoolwork (56,5%). Overall, respondents indicate a strong awareness in the knowledge domain. For attitudes towards internet use, 63% "Agree" that it can be risky to download files on their school computer, there was a slight difference between "Strongly agree" (47,8%) and "Agree" (44,6%) for accessing certain websites at school, and most "Strongly agree" that it does not matter what information one puts on a website, even if it helps them in doing their schoolwork (55,4%). The overall attitude indicates strong awareness, and the respondents indicate a better attitude compared to knowledge. For behaviour, the majority "Disagree" (41,3%) with the statement that they download any files that helps them with their schoolwork. Similarly, most "Disagree" (38%) that they visit any websites that they want to when they are at school. When asked whether they assess the safety of a website before entering any information, 48% responds "Strongly agree", and 42,4% "Agree" with this statement. The overall behaviour indicates good awareness of internet use, however, similar to e-mail, behaviour has a lower score compared to knowledge and attitude.

In summary, respondents indicate a strong awareness in regards to internet use, where they score the highest on knowledge and attitude, and where their attitude scores the highest. When performing an Independent Samples t-Test, and 4 questions are shown to not display equal variance. Of these 4 questions, 3 of them has a p-score that indicates that they are significant. The Independent Samples t-Test for these questions are shown in figure 5.9.

Independent Samples Test for Internet use

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
While I am at school, I should not access certain websites	Equal variances assumed	5.774	.018	2.213	90	.029	.43404	.19617	.04431	.82378
	Equal variances not assumed			2.195	77.748	.031	.43404	.19772	.04040	.82768
If it helps me do my schoolwork, it does not matter what information I put on a website	Equal variances assumed	5.785	.018	1.819	90	.072	.33191	.18249	-.03063	.69446
	Equal variances not assumed			1.799	69.601	.076	.33191	.18452	-.03613	.69996
I download any files onto my school computer that will help me do my schoolwork	Equal variances assumed	6.857	.010	2.914	90	.005	.68889	.23642	.21920	1.15857
	Equal variances not assumed			2.906	87.579	.005	.68889	.23706	.21776	1.16002
When accessing the internet at school, I visit any website that I want to	Equal variances assumed	10.395	.002	2.858	90	.005	.63972	.22384	.19502	1.08442
	Equal variances not assumed			2.838	79.759	.006	.63972	.22540	.19113	1.08831

Figure 5.9: Independent samples t-test for internet use

From the above presented figure, we can observe that the question "While I am at school, I should not access certain websites" has a significance of .031 < .05, which indicates that the differences are statistically significant. Figure 5.10 shows the difference in answers between technical and non-technical students for this particular question.

From the above presented figure, we can observe that students associated with a non-technical faculty tends to disagree more with the given statement. This indicates that students affiliated with a technical faculty has better knowledge in terms of accessing websites at school.

The next question states "I download any files onto my school computer that

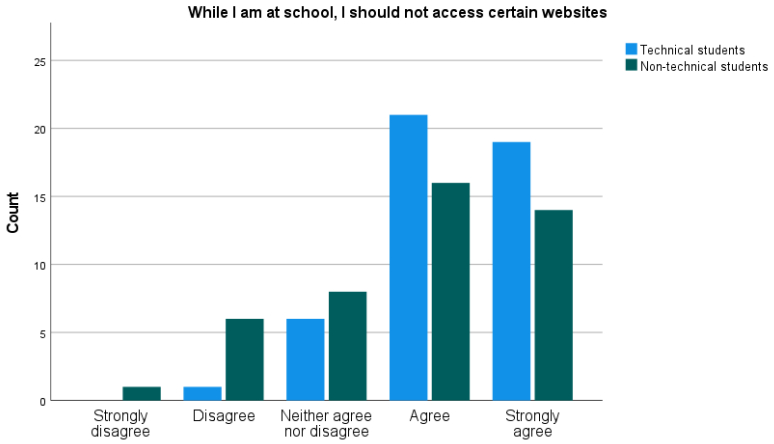


Figure 5.10: Knowledge difference between technical and non-technical students

will help me do my schoolwork", and observing from figure 5.9, the p-value is .005 $<$ .05, thus, the difference is significant. From figure 5.11, we can observe that non-technical students report that they are more agreeable towards the proposed question.

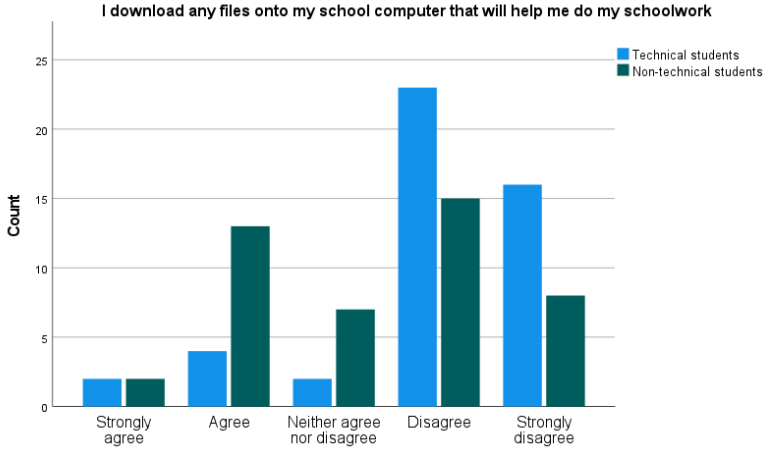


Figure 5.11: Difference in downloading files between technical and non-technical students

The last question with a statistical significant result (.006 $<$ .05), asked the participants "When accessing the internet at school, I visit any website that I want to". Comparing the results between technical and non-technical students, we can observe from figure 5.12 that non-technical students tend to be more agreeable and indifferent towards visiting any website while being at school, while technical students indicate that they do not agree with this statement.

To summarise the results from internet use, the overall results indicate that

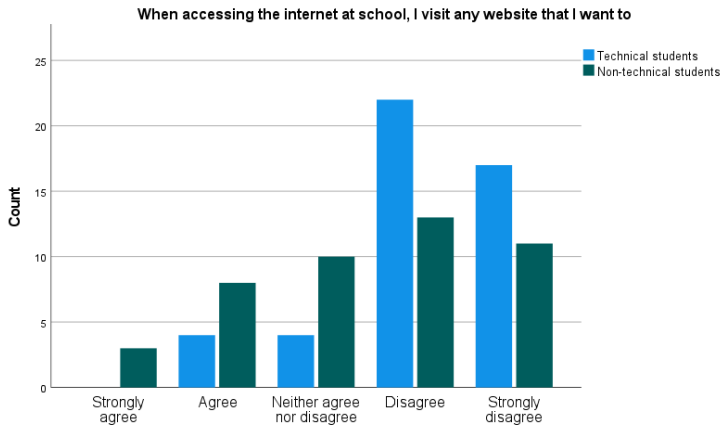


Figure 5.12: Difference in accessing websites between technical and non-technical students

the security awareness is good, however, knowledge and attitude shows a slightly higher score compared with behaviour. Comparing technical and non-technical students, technical students displays a greater knowledge and behaviour in terms of accessing websites while being at school.

5.4.4 Mobile devices

The section for mobile devices asks questions regarding phone passcode, remote wipe, and shoulder surfing [1]. When presented with the statement "The passcode on my phone should not be personal information that is publicly available", the majority strongly agreed with this statement (54,3%). When asked whether respondents think that they should have remote wipe enabled on their phone, 41,3% reported indifference, while 28,3% and 23,9% reported that they "Agree" and "Strongly agree", respectively. The last knowledge question asked whether they ensure that strangers cannot see their screen when they are working on a sensitive document, and 47,8% answered that they "Strongly agree" with this statement. When asked about their attitudes, 58,7% "Strongly agree" that it is risky to have their own birth year as a passcode on their phone. 34,8% indicated indifference whether they think it is risky to not have remote wipe enabled on their phone, however, slightly fewer also indicates that they "Agree" with this statement (32,6%). Lastly, the participants were asked whether they think that it is risky to access documents with sensitive information on a laptop if strangers can see the screen, and the majority (47,8%) "Agree" with this statement. Regarding behaviour, most participants (64,1%) indicate that they do not use their birthday or other publicly available information about themselves as their passcode on their phone, while 22,8% and 28,3% answered that they "Strongly disagree"

[1] Shoulder surfing is the act of observing other people's information without their consent [25]

Group Statistics[a]

	faculty_group	N	Mean	Std. Deviation	Std. Error Mean
The passcode on my phone should not be personal information that is publicly available (e.g. date of birth)*	Technical students	47	4.3404	.84124	.12271
	Non-technical students	45	4.3111	1.06221	.15834
I should have remote wipe of my phone enabled*	Technical students	47	3.7021	.85757	.12509
	Non-technical students	45	3.6667	1.02247	.15242
When working on a sensitive document, I must ensure that strangers cannot see my laptop screen*	Technical students	47	4.3191	.72551	.10583
	Non-technical students	45	4.2667	.91453	.13633
It is risky to have my birth year as my phone's passcode**	Technical students	47	4.4468	.80240	.11704
	Non-technical students	45	4.4222	.81153	.12098
It is risky to not have remote wipe enabled on my phone**	Technical students	47	3.6170	.82233	.11995
	Non-technical students	45	3.6000	1.11600	.16636
It is risky to access documents with sensitive information on a laptop if strangers can see my screen**	Technical students	47	4.2553	.73627	.10740
	Non-technical students	45	4.1778	.74739	.11141
I use my birthday or other publicly available information about myself as a passcode on my phone***	Technical students	47	4.3617	1.03052	.15032
	Non-technical students	45	4.3556	1.11101	.16562
I have remote wipe of my phone enabled***	Technical students	47	2.7234	1.33028	.19404
	Non-technical students	45	2.6000	1.40454	.20938
I check that strangers cannot see my laptop screen if I am working on a sensitive document***	Technical students	47	4.2340	.91397	.13332
	Non-technical students	45	4.0667	.93905	.13999

Figure 5.13: Group statistics for mobile devices

and "Disagree" that they have enabled remote wipe on their phone, while only 5,4% (Agree) and 17,4% (Strongly agree) indicated that they have. The last question asked whether respondents check if strangers can see their laptop screen before working on a sensitive document, where the majority of responses were split 41,3% between "Agree" and "Strongly agree".

Performing an Independent Samples t-test yielded only a single question that was significant in Levene's test, however, observing the p-value for this question indicates that it was no significant value ($.934 > .05$). By observing the group statistics displayed in figure 5.13 for mobile devices, we can observe that the mean scores are generally high, however, the score drops to 2 when asked whether they have enabled remote wipe on their phone.

To summarise, the overall awareness of mobile devices has a good score, although, participants indicate indifference and disagreement with remote wiping of mobile devices, regardless whether they are technical or non-technical students.

5.4.5 Information handling

The section for information handling asks respondents about dealing with sensitive print-outs and plugging an unknown USB stick into their school computer. For the knowledge section, when asked whether sensitive print-outs can be disposed of in the same manner as non-sensitive ones, 55,4% and 40,2% answered "Strongly agree" and "Agree", respectively. 62% indicated that they "Strongly disagree" that one should not plug an unknown USB stick into their school computer, and 62% "Strongly disagree" that print-outs with sensitive information can be left in classrooms/meeting rooms overnight. For attitudes, 51,1% said that they "Strongly disagree" with the statement that print-outs can be disposed of in the rubbish bin, 66,3% "Strongly disagree" that nothing bad can happen when an unknown USB is plugged into their school computer, and 56,5% indicate that they "Strongly agree" that it is risky to leave print-outs with sensitive information in classrooms/meeting rooms overnight. For behaviour, 42,4% and 39,1% report that they "Strongly agree" and "Agree" that they ensure print-outs are shredded or destroyed when disposed of; 59,8% indicate say that they "Strongly agree" that they would not plug an unknown USB into their school computer, and 68,5% say that they "Strongly disagree" that they would leave print-outs with sensitive information in classrooms/meeting rooms when they are not there.

Performing an Independent Samples t-Test shows that one of the behavioural questions refutes Levene's equal variance, and the p-score for this element is .003 $<$ .05, meaning that the difference is significant. Figure 5.14 shows the result for this particular question.

Independent Samples Test for Information handling

	Levene's Test for Equality of Variances		t-test for Equality of Means						
								95% Confidence Interval of the Difference	
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
I leave print-outs that contain sensitive information in classrooms/meeting rooms when I am not there	25.241	.000	3.177	90	.002	.63168	.19882	.23670	1.02666
			3.121	52.525	.003	.63168	.20241	.22561	1.03775

Figure 5.14: Group statistics for mobile devices

Looking at the distribution between technical and non-technical students, we can observe that the non-technical students tend to answer more spread, and they indicate that they either are indifferent, or that they do leave print-outs with sensitive information in classrooms/meeting rooms when they are not there. The distribution of these answers are visualised in figure 5.15.

In summary, the overall awareness for information handling is very good, however, students from a technical faculty displays better behaviour than non-technical students, when it comes to leaving print-outs with sensitive information.

5.4.6 Incident reporting

This section concerns reporting suspicious e-mails, ignoring poor security behaviour, and reporting of security incidents/discrepancies. To the first statement "If

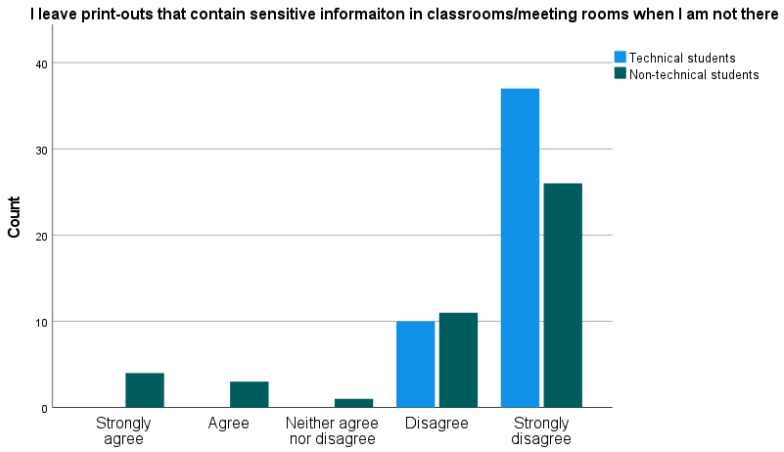


Figure 5.15: Distribution of information handling behaviour

I receive a suspicious e-mail on my school account, I must report it", 44,6% said that they "Agree", and 22,8% indicated indifference. Regarding ignoring poor security behaviour of classmates, 53,3% and 28,3% answered that they "Agree" and "Neither agree nor disagree", respectively. When asked whether they think that reporting a security incident/discrepancy is optional, 37% indicated that they are indifferent, and 32,6% said that they "Disagree" with this statement. When asked what participants think about these statements, 37% "Disagree" that nothing bad can happen if they ignore a suspicious e-mail, while 23,9% and 20% report that they are indifferent and that they "Agree", respectively. When asked whether they think that nothing bad can happen if they ignore poor security behaviour by their classmates, most respondent say that they "Disagree" (48,9%). The last question on attitude was whether they think that it is risky to ignore security incidents, even if they think they are not significant, and the majority of respondents (59,8%) answered that they "Agree" with this statement. Regarding behaviour, 32,6% answered "Agree" that they would ignore a suspicious e-mail, while 27,2% indicated that they "Disagree". When asked whether they would take action if they saw a classmate ignoring security rules, the majority reported that they were indifferent (40,2%), but 34,8% reported that they "Agree". The final behavioural statement asked if respondents would report any security incident/discrepancy if they noticed; 31,5% reported that they were indifferent, while 42,4% said that they "Agree".

Performing an Independent Samples t-Test showed no significant variance between technical and non-technical students, and thus, there is no statistical significant difference between these groups for incident reporting. Overall, the level of awareness for incident reporting shows a general lower score for each category, and the results indicate a bigger indifference for this particular dimension. An overview of the mean scores for each category and each question is presented

in the group statistics in figure 5.16.

Group Statistics for Incident reporting[a]

	faculty_group	N	Mean	Std. Deviation	Std. Error Mean
If I receive a suspicious e-mail on my school account, I must report it*	Technical students	47	3.7447	.89608	.13071
	Non-technical students	45	3.8444	.97597	.14549
I must not ignore poor security behaviour by my classmates*	Technical students	47	3.8723	.64663	.09432
	Non-technical students	45	3.5778	.89160	.13291
It's optional to report security incidents/security discrepancies*	Technical students	47	3.4468	.92803	.13537
	Non-technical students	45	3.2444	1.04785	.15620
If I ignore a suspicious e-mail on my school account, nothing bad can happen**	Technical students	47	3.4894	1.13965	.16623
	Non-technical students	45	3.4000	.98627	.14702
Nothing bad can happen if I ignore poor security behaviour by a classmate**	Technical students	47	4.0426	.85865	.12525
	Non-technical students	45	3.8667	.81464	.12144
It's risky to ignore security incidents, even if I think that they are not significant**	Technical students	47	3.9149	.71717	.10461
	Non-technical students	45	3.7778	.76541	.11410
If I receive a suspicious e-mail on my school account, I would ignore it***	Technical students	47	3.0000	1.25109	.18249
	Non-technical students	45	2.6667	1.18705	.17696
If I noticed my classmate ignoring security rules, I would not take any action***	Technical students	47	3.4255	.80067	.11679
	Non-technical students	45	3.1778	1.11373	.16603
If I noticed a security incident/security discrepancy, I would report it***	Technical students	47	3.4681	.85595	.12485
	Non-technical students	45	3.4000	1.00905	.15042

a. *Knowledge, **Attitude, ***Behaviour

Figure 5.16: Group statistics for incident reporting

5.4.7 Computer security

The final dimension poses questions about updating the school computer and its applications, anti-virus, and usage of a virtual private network (VPN). In the knowledge dimension, the first presented question was "I must ensure that my school computer and its applications are always updated". Half of respondents answered that they "Agree", while 27,2% were indifferent. The next question asks whether one should always have an anti-virus application on their school computer; most respondents "Agree" to this statement (30,4%), while 27,2% were indifferent. The last question asked whether one should always use a VPN when connected to a guest network outside of NTNU; the majority (31,5%) responded that they were indifferent, and 29,3% "Agree" with this statement. For attitude, above half of respondents (57,6%) "Agree" that it is risky to postpone pending updates, while 20,7% responded indifferently. When asked whether they think it is risky to not have an anti-virus application, 37% "Agree", and 25% "Strongly agree". For the last attitude question, which states that nothing bad can happen if a VPN is not used when connected to a guest network outside NTNU, 37% "Disagree", while

32,6% is undecided. For behaviour, 35,9% "Disagree" that they postpone pending updates, while 21,7% and 22,8% report that they "Strongly disagree" and "Agree", respectively. 28% "Strongly disagree" that they do not have an anti-virus application, while 22,8% "Disagree", 20% "Agree", and 15% "Strongly agree" to this statement. The last question asks whether respondents do not utilise a VPN when they are connected to a guest network outside NTNU. 32,6% are undecided, 23,9% "Agree", and 22,8% "Agree" to this statement.

Performing an Independent Samples t-Test resulted in no significant variance between technical and non-technical students, meaning that there is no statistical difference between these groups for the computer security dimension. The overall results indicate a security awareness of a lower score than compared to other dimension, however, a majority of answers were also undecided for this particular dimension. The mean scores for each question is presented in the group statistics in figure 5.17.

Group Statistics[a]

	faculty_group	N	Mean	Std. Deviation	Std. Error Mean
I must ensure that my school computer and its applications are always updated*	Technical students	47	3.7447	.76522	.11162
	Non-technical students	45	3.5556	.94281	.14055
I must have an anti-virus application on my school computer*	Technical students	47	3.5532	1.17600	.17154
	Non-technical students	45	3.6000	1.13618	.16937
I should always use a VPN when I am connected to a guest network outside of NTNU*	Technical students	47	3.3404	1.14733	.16736
	Non-technical students	45	3.3778	1.13396	.16904
It is risky to postpose pending updates for my school computer and its applications**	Technical students	47	3.8298	.76098	.11100
	Non-technical students	45	3.7111	.86923	.12958
It is risky to not have an anti-virus application on my school computer**	Technical students	47	3.6596	1.04832	.15291
	Non-technical students	45	3.7111	1.12052	.16704
Nothing bad can happen if I do not use a VPN when I am connected to a guest network outside of NTNU**	Technical students	47	3.7872	.95408	.13917
	Non-technical students	45	3.4889	.92004	.13715
I postpone pending updates on my computer and its applications***	Technical students	47	3.5745	1.11793	.16307
	Non-technical students	45	3.2889	1.35885	.20256
I do not have an anti-virus application***	Technical students	47	3.4255	1.36326	.19885
	Non-technical students	45	3.1333	1.54626	.23050
When I am connected to a guest network outside of NTNU, I do not use a VPN***	Technical students	47	3.2128	1.15976	.16917
	Non-technical students	45	2.8000	1.09959	.16392

a. *Knowledge, **Attitude, ***Behaviour

Figure 5.17: Group statistics for computer security

Chapter 6

Discussion

This section aims to present and discuss the aforementioned research questions in relation to the obtained results from the previous chapter. This chapter will be presented such that each research question is presented, followed by an interpretation of the associated results, in terms of what they mean or what they can indicate.

6.0.1 General information

Students were asked whether they knew how to report a security incident, a security discrepancy, and whether they have completed the security course, and if they knew that NTNU provided such as course. The distribution between students were very similar, independent of their associated faculty. The common denominator, however, is that very few answered "Yes" on any of the questions, which suggests that the course is not well known by students, and very few indicate that they know how to report a security incident/discrepancy.

6.1 How knowledgeable are student at NTNU with information security concepts related to the university's policies and guidelines?

6.1.1 Password management

Overall, the displayed security knowledge of students in regards to password management indicates a good awareness, for both technical and non-technical students. Above half of respondents (52,2%) strongly agrees that passwords from their social media should not be re-used, however, a fair portion of the remaining answers (29,3%) only agrees with this. A possible explanation for this might be that an individual might initially regard their password secure, and therefore choose to re-use it. A special publication by NIST [1] discusses the creation of pass-

[1] https://pages.nist.gov/800-63-3/sp800-63b.html

words, and states that the length of a password is one of the primary factors of a secure password. It is also stated that by having individuals remember complex passwords, it is more likely that the password is written down or stored in an infeasible manner. This might also explain why there is a split between students on the matter of using a mix of letters, numbers, and special characters in their school passwords (42,4% agree vs. 40,2% agree). For sharing passwords, 73,9% indicated a strong disagreement that it is an acceptable practice, with an equal distribution between both technical and non-technical students.

6.1.2 E-mail use

The overall result indicates that the student's knowledge of e-mail use is sufficient. 83,7% report that one should be careful in clicking on any links in e-mails, and 75% reports that sending sensitive information in e-mails without encrypting the contents first is unacceptable. When asked if they receive an e-mail with sensitive content, and whether they should delete the sensitive content, the results indicate a stronger indecisiveness compared to the two aforementioned question (32,6%), A likely explanation for this result might be that students typically do not handle information that can be regarded as sensitive or confidential, and therefore it might be interpreted as not relevant, or simply that they do not know.

6.1.3 Internet use

71 respondents (77,1%) indicate apprehensiveness for downloading files onto one's computer, even if they believe that the files will help them in their schoolwork. 70 respondents (76%) also indicated apprehensiveness in visiting certain websites when one is at school, and 87 students (94,5%) showed positive knowledge against sharing information with websites, even if it would help them in their schoolwork. What is worth mentioning, is the distribution for the reported answers given when asked if there are certain websites that one should not visit. Of those who reported uncertainty, 57,1% of these were non-technical students; additionally, of those who reported disagreement with this particular question, 87,5% of these reports were non-technical students. This suggests that students with associated with non-technical faculties shows a lower knowledge of internet use awareness, and in this case, would be more likely to access malicious websites than compared to a technical student.

6.1.4 Mobile devices

81 respondents (88%) agrees that a phone passcode should not be publicly available information, however, 38 respondents (41,3%) are undecided whether remote wiping of one's phone should be enabled, where 23 (60,5%) of these were technical students. Why there is such an amount of undecided answers might be due to respondents not understanding the question, as there is no explanation of what remote wiping means, or it could simply indicate that they do not know

whether it should be enabled or not. Lastly, 72 respondents (78,2%) agrees that one should check whether anyone can see their screen when working on a sensitive document. The overall knowledge of mobile devices can be considered as good, as the scores are generally high for both groups, apart from being undecided on whether remote wiping of their phone should be enabled or not.

6.1.5 Information handling

The overall knowledge of handling information is generally very high, where 84,7% reported that they disagree with disposing print-outs with sensitive contents in the same way as non-sensitive ones, 93,4% agrees that one should not plug an unknown USB stick into their computer, and 96,7% disagrees that print-outs with sensitive information should be left in a classroom or study room overnight. Also in this case, there were no significant difference between technical and non-technical students.

6.1.6 Incident reporting

When asked what one should do if they receive a suspicious e-mail on their school e-mail, the majority of students think it should be reported (67,3%), however, 28,3% report that they are undecided. A possible explanation could be that there is a variance in how "suspicious" is interpreted by the respondents; where one might think of this as directly phishing, one could also regard a suspicious e-mail as simply an e-mail that was sent to the wrong person. Out of the respondents that strongly indicated that is must be reported, 61,9% were from non-technical students. 61 respondents (66,3%) agree that poor security behaviour from classmates must not be ignored, while 26 respondents (28,2%) suggested that they were indifferent, which might indicate the same problem as in the previous question, where this might be a result of not enough information as to what poor security behaviour is. When asked whether they think reporting a security incident or discrepancy is optional, surprisingly, only 41 respondents (44,5%) suggested that they think it is. Out of the remaining respondents, 52 respondents (52,1%) reported to be indifferent, and 17 respondents (18,4%) believe that it is optional. From those who reported that they were indifferent or believe that it is optional, 54,9% of these respondents were non-technical students. The overall knowledge of incident reporting can be summarised as decent, where respondents generally indicate that they have good knowledge, however, there are some discrepancies, especially regarding ignoring security behaviour of others, and the reporting of security incidents and discrepancies. The knowledge of incident reporting suggests that non-technical students have slightly less knowledge of reporting incidents than compared to technical students.

6.1.7 Computer security

The overall computer security knowledge of students suggests sufficient knowledge, where most participants indicate that one should ensure that their computer and its applications are always updated (63%), and that one must have an anti-virus application (55,4%). It seems, however, that there is some disagreement and indifference when asked about using a VPN; 31,5% of respondents reports to be indifferent, and 21,8% disagrees that VPN should be used when connected to a guest network outside of NTNU. It is likely that the reason for this distribution is caused by the wording of the question and/or the lack of clarification, where it is not specified what a VPN is, or what it is used for. Looking at the difference between technical and non-technical students, 58,6% of indifferent reports, and 55% of reports that disagree with the statement are from technical students.

6.2 What are student's attitude towards information security concepts related to the university's policies and guidelines?

6.2.1 Password management

The attitudes towards password management is generally very high, where the majority of students who disagrees with that it is safe to re-use a password for social media for their school accounts are technical students (52,5%). The same is also true for the attitude towards sharing passwords with classmates, where technical students make up 52,8% of respondents that indicates disagreement. Considering that there are an additional two respondents for technical students, the significance is not enough to tell anything about the difference between the groups, as they are fairly equally split. The opposite situation occurs on the last question when asked about having a password consisting of just letters. Of the respondents indicating that this is not sufficient, 51,6% of these are non-technical students. There is, however, worth mentioning that there seems to be reported a higher amount of indifference for this question. This is in line with the results for respondent's knowledge about password management, and it might be speculated that this is due to the same reasons as described earlier.

6.2.2 E-mail use

The reported attitudes towards e-mail use is generally very good; 85 participants (92,3%) reported that they think it is unsafe to click links in e-mails, and 79 (85,8%) indicated that it is risky to send sensitive information without encrypting the contents first. In line with the reported knowledge for e-mail use, when asked about deleting sensitive content before replying or forwarding an e-mail, there is a noticable amount of respondents that indicate indifference (28,3%), and it would

be fair to assume that the reasons for this are the same as the ones described in the knowledge-section for e-mail use.

6.2.3 Internet use

The attitudes towards internet use is also indicated to be very sufficient. 88% report that they agree with downloading files can pose a risk, 92,2% of respondents report that they agree that a website is not necessarily safe, even though it is accessible while being at school, and 88% report that entering information into a website can pose a risk. The attitudes towards internet use also line up with the results from the knowledge-section, where there is a significant amount of non-technical students who display indifference in regards to accessing websites at school (85,7%).

6.2.4 Mobile devices

There seems to be a strong agreement that it is risky to have one's birth-year as a passcode on their phone (89,1%), however, the majority display an indifference when asked whether they think that not having remote wiping enabled poses a risk (34,8%). This is the same case as for the knowledge-section, and is also probably a result of the problems that are presented in the previous section.

6.2.5 Information handling

The attitudes for information handling shows a close resemblance with the overall result presented for knowledge within this dimension, where attitudes for all questions shows a sufficient level, and where there is no significant difference between technical and non-technical students.

6.2.6 Incident reporting

Just above half of respondents believes that it can pose a risk to ignore a suspicious email (53,2%), where the distribution between technical and non-technical students are closely split. This is also the case for those who reported that ignoring a suspicious e-mail does not pose a risk, which suggests that there is no difference between the student groups.

6.2.7 Computer security

There seems to be a higher indifference for attitudes towards computer security. The question that is reported with the highest amount of indifference is whether there is a risk associated with not using a VPN when connected to a guest network outside NTNU (32,6%). Similar to the aforementioned assumption, it is likely that the amount of indifference is due to a lack of explanations.

6.3 How does student's security behaviour compare with the expected behaviour related to the university's policies and guidelines?

6.3.1 Password management

The reported password management behaviour is in line with the previously reported knowledge and attitude, where there is a strong agreement that respondent use different passwords for their school accounts (85,8%), and strong agreement that students never share their passwords with classmates (97,8%). What differs from the previously reported knowledge and attitude, is the lack of indifferent and disagreeing answers. There has previously been a split between reports on this subject when measuring knowledge and attitude, however, for behaviour, 86,9% report that they use a combination of letters, numbers, and special characters for their passwords. This could indicate that the two previously questions were asked in a manner that made the question hard to understand, however, it might be more likely that this is a result of social desirability bias

6.3.2 E-mail use

Reported behaviour for e-mail use indicates a strong indifference in regards to sending sensitive information without encrypting the content, and deleting sensitive content before forwarding or replying to an e-mail. As previously mentioned, this might be due to students not having experienced these scenarios, and thus, the indifference could be a result of not knowing how they would react.

6.3.3 Internet use

A surprising result, is the number of respondents who report that they download any files that they believe will help them in their schoolwork. A total of 17 respondents (18,5%) said that they download any files, and 71,4% of these respondents are non-technical students, which suggests that these students are most likely to download malicious files. There is a similar result when asked whether respondents visit any site that they want to, where 16,3% reported that they do, and of these students, 73,3% are also non-technical students. This suggests that non-technical students are also the most likely to visit malicious websites. Somewhat contrary to these results, almost half of students who report that they assess the security of websites before entering any information are also non-technical students (46,4%).

6.3.4 Mobile devices

Behaviour regarding mobile devices is similar to reported knowledge and attitude, however, there are more respondents reporting that they have not enabled

remote wipe of their devices (28,3%), where the split between technical and non-technical are roughly evenly distributed. This could suggests that the reported indifference in the previous sections indicate that respondents are unaware of the risks of not having remote wipe enabled, in contradiction to not knowing what it is.

6.3.5 Information handling

Reported behaviour in information handling follows the same patterns as the reported knowledge and attitude dimensions, and the overall behavioural awareness is suggested to be at a feasible level.

6.3.6 Incident reporting

Almost half of respondents reported that if they received a suspicious e-mail on their school e-mail, they would ignore it (46,7%). From those who reported that they would ignore the e-mail, there is an almost equal split between technical and non-technical students. It might be fair to assume that this particular question has been answered based on the best-practice of managing one's own personal e-mail, and the results suggests that it is likely that neither technical nor non-technical students would report such an incident. There is also a strong indifference in regards to taking action if they observe a classmate ignoring security rules. As previously stated, this might be due to a poorly-worded question rather than indifference in taking action. Contradictory to the first question, most respondents report that if they noticed a security incident/discrepancy, they would report it (52,2%). It is also worth mentioning that 31,5% indicated indifference to this question, which could suggest that students do not know how to report a security incident/discrepancy.

6.3.7 Computer security

57,6% of students suggest that do not postpone updates on their computer and its applications. Comparing the student groups, technical students display a slight better behaviour than compared to non-technical students, however, not significantly. When asked whether respondents have anti-virus, only slightly above half report that they have anti-virus software (51%), 35,9% say that they do not have anti-virus, and 13% are undecided. Considering that anti-virus is built-in software that comes with standard Windows, there is a chance that this question might have been interpreted as having an active subscription, purchased, or downloaded additional software in addition to the standard anti-virus (such as AVG, McAfee, F-secure etc.). It could also suggest that respondents do not know whether they have anti-virus, and would therefore answer indifferently. Of those who answered that they do not have anti-virus installed, 60,6% are non-technical students, which could suggest that non-technical students are more likely to not be aware if they have anti-virus installed or not. When asked whether students use a VPN when

connected to a guest network outside of NTNU, there is a split between 33,7% that say they do, and those who do not. The remaining answered indifferently. Of those who answered that they use a VPN, 67,7% are technical students, while for those who answered that they do not use a VPN, 58% were non-technical students. This suggest that technical students have better behaviour compared to non-technical students in regards to using a VPN when connected to a guest network outside of NTNU.

6.4 Summary

The findings from the result can be summarised as the following:

- Overall password management awareness is sufficient, however, knowledge and attitude differ slightly from behaviour, where reported self-reported behaviour shows a greater awareness.
- Overall e-mail use awareness is good, however, some questions gave indifferent answers, indicating that there might be a need for increased awareness.
- Overall internet use awareness is good, however, non-technical students indicate that they are more prone to visit any website and download any files than compared to technical students.
- Overall mobile devices awareness is good, however, respondents showed indifference to remote wiping of phone, and most did not have this feature enabled
- Overall, information handling awareness is very sufficient
- Incident reporting shows differences between dimensions. Most believe there is a risk to ignoring a suspicious e-mail, but indicate that they would ignore a suspicious e-mail if they received one.
- Computer security awareness is generally sufficient, however, many were indifferent on the use of VPN. Technical students showed a slightly better awareness on VPN usage and anti-virus compared to non-technical students.

As suggested by [2], it seems that knowledge and attitude are closely related, as they tend to have equal values. Behaviour, however, tends to go have more variance, and as indicated by [13] - assessing behaviour through self-reporting is not feasible for obtaining actual behaviour, but rather to obtain a general sense of participant behaviour.

Chapter 7

Conclusion

The purpose of this study was to determine the level of security awareness among students at NTNU. The study was conducted through an online questionnaire, and aimed to investigate three dimensions of security awareness, namely - Knowledge, Attitude, and Behaviour. Students were asked to self-report their knowledge, attitudes, and behaviour in regards to common human errors identified in the security training that NTNU provides to its students. The questionnaire was distributed through various platforms, specifically targeting students at NTNU.

The knowledge level of students is indicated to be at a sufficient level, where identified likely points for improvement includes knowledge of sensitive and confidential information in e-mails, downloading files and visiting websites, remove wiping of mobile devices, incident reporting, usage of VPN, and anti-virus.

The attitude level of students is also indicated to be on a sufficient level, where identified likely points for improvement includes better attitudes towards sensitive and confidential content in e-mails, internet use, remote wiping of mobile devices, suspicious e-mails, and usage of VPN.

The behaviour level of students is has also been shown to be on a sufficient level, where identified likely points for improvement includes better behaviour in regards to sensitive and confidential content in e-mails, downloading files and visiting websites, remote wiping of mobile devices, reporting of security incidents, usage of VPN and anti-virus.

The overall results also suggest that students that are affiliated with a technical faculties display slightly better awareness in internet use and computer security, however, it should not be considered conclusive, considering the sample size and the overall population.

Lastly, this thesis can be considered as a novelty contribution towards further assessing the security awareness of students at NTNU. As stated above, this thesis should not be considered as a foundation for future work, but rather as a general direction in which can be used to assess and increase the awareness of students at NTNU.

Chapter 8

Limitations and Future Work

8.1 Limitations

The main limitation of this study lies on the obtained sample size. The total obtained usable sample size for this project was N = 92, which is insufficient, as we want to describe a population of roughly 42000 [1]. There might have been multiple reasons for why a sufficient sample size was not obtained; (1) There is no efficient way of reaching out to students besides direct contact through e-mail, and the task of obtaining enough responses was greatly underestimated; (2) The response rate for this particular project was very low (only 5%), which might have been the result of students practicing for exams and conducting their own research during this same time period; (3) For the first two weeks of distribution, students were required to log in with their school account in order to answer the survey, which might have turned down a considerable amount of potential participants. The initial reason for requiring student login was due to ensuring that participants actually were students, however, it was decided between the author and supervisors that since the survey was only distributed on channels targeted towards students, a control question in the beginning of the survey would be sufficient enough.

Another factor that can be considered a limitation of this study could be the questionnaire itself. At the end of the survey, respondents were able to give feedback. A majority of the received feedback indicated that there were too many questions, that the questions were too similar, and that the questions were worded either too leading or that there were too many grammatical negations, which made them harder to understand. Some also suggested that some questions should have been "Yes/No" instead of a scale.

[1] Number is rounded and taken from https://www.ntnu.no/tall-og-fakta

8.2 Future work

Future work should consider the limitations described above, as well as taking the provided feedback into account as well. Future work in a similar area would not only be beneficial for NTNU in strengthening their security culture and an important factor in continually improving their awareness training, but also beneficial for the students themselves. It would be interesting to see a study with a bigger and more representative sample, and see whether there are any differences between faculties, departments, and educational levels.

Bibliography

[1] N. Hänsch and Z. Benenson, 'Specifying it security awareness,' in *2014 25th International Workshop on Database and Expert Systems Applications*, IEEE, 2014, pp. 326–330.

[2] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac and T. Zwaans, 'The human aspects of information security questionnaire (hais-q): Two further validation studies,' *Computers & Security*, vol. 66, pp. 40–51, 2017.

[3] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann and B. Hohler, 'Employees' information security awareness and behavior: A literature review,' in *2013 46th Hawaii International Conference on System Sciences*, IEEE, 2013, pp. 2978–2987.

[4] F. A. Aloul, 'The need for effective information security awareness,' *Journal of advances in information technology*, vol. 3, no. 3, pp. 176–183, 2012.

[5] J. Leach, 'Improving user security behaviour,' *Computers & Security*, vol. 22, no. 8, pp. 685–692, 2003.

[6] S. M. Furnell, N. Clarke and D. Lacey, 'Understanding and transforming organizational security culture,' *Information Management & Computer Security*, 2010.

[7] I. Legárd *et al.*, 'Building an effective information security awareness program,' *Central and Eastern European eDem and eGov Days*, vol. 338, pp. 189–200, 2020.

[8] E. B. Kim, 'Recommendations for information security awareness training for college students,' *Information Management & Computer Security*, 2014.

[9] Y. Rezgui and A. Marks, 'Information security awareness in higher education: An exploratory study,' *Computers & Security*, vol. 27, no. 7-8, pp. 241–253, 2008.

[10] S. Hina and D. D. Dominic, 'Information security policies: Investigation of compliance in universities,' in *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)*, IEEE, 2016, pp. 564–569.

[11] S. Hina and P. D. D. Dominic, 'Information security policies' compliance: A perspective for higher education institutions,' *Journal of Computer Information Systems*, 2018.

[12] J. B. Ulven and G. Wangen, 'A systematic review of cybersecurity risks in higher education,' *Future Internet*, vol. 13, no. 2, p. 39, 2021.

[13] H. A. Kruger and W. D. Kearney, 'A prototype for assessing information security awareness,' *Computers & security*, vol. 25, no. 4, pp. 289–296, 2006.

[14] K. Parsons, A. McCormac, M. R. Pattinson, M. A. Butavicius and C. Jerram, 'An analysis of information security vulnerabilities at three australian government organisations.,' in *EISMC*, 2013, pp. 34–44.

[15] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson and C. Jerram, 'Determining employee awareness using the human aspects of information security questionnaire (hais-q),' *Computers & security*, vol. 42, pp. 165–176, 2014.

[16] E. B. Kim, 'Information security awareness status of business college: Undergraduate students,' *Information Security Journal: A Global Perspective*, vol. 22, no. 4, pp. 171–179, 2013.

[17] A. P. Filippidis, C. S. Hilas, G. Filippidis and A. Politis, 'Information security awareness of greek higher education students—preliminary findings,' in *2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, IEEE, 2018, pp. 1–4.

[18] G. Törley, 'The level of information security awareness of first-year university students,' CEUR Workshop Proceedings, 2020.

[19] A. F. Firmansyah, Q. Aini, A. Saehudin, S. Amsariah *et al.*, 'Information security awareness of students on academic information system using kruger approach,' in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, IEEE, 2020, pp. 1–7.

[20] G. Kiss, 'The information security awareness of the slovakian kindergarten teacher students at starting and finishing the study in higher education,' in *SHS Web of Conferences*, EDP Sciences, vol. 66, 2019, p. 01 042.

[21] C. P. Garrison and O. G. Posey, 'Computer security awareness of accounting students,' in *Southwest Decision Sciences Thirty-Sixth Annual Meeting*, 2006.

[22] G. Wangen, E. Ø. Brodin, B. H. Skari and C. Berglind, 'Mørketallsundersøkelsen ved ntnu 2018,' 2019.

[23] J. N. Ellestad, M. L. Lilja, A. G. Gustad and E. S. Skuggerud, 'Sikkerhetskultur ved ntnu,' B.S. thesis, NTNU, 2019.

[24] I. M. A. G. Azmi, Q. M. Ashraf, S. Zulhuda and M. B. Daud, 'Critical data leak analysis in educational environment,' in *2016 4th International Conference on Cyber and IT Service Management*, IEEE, 2016, pp. 1–6.

[25] M. Eiband, M. Khamis, E. Von Zezschwitz, H. Hussmann and F. Alt, 'Understanding shoulder surfing in the wild: Stories from users and observers,' in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017, pp. 4254–4265.

Appendix A

Questionnaire

Security culture among students at NTNU

Side 1

Introduction

Security awareness, in the context of this study, is used to describe the combination of security knowledge, attitude towards security, and security behaviour. By security knowledge, it is meant the individual's knowledge regarding security concepts and how they work. By attitude towards security, the individual's feelings towards security is considered. By security behaviour, it is meant the actions that an individuals takes in order to prevent security incidents and/or security deviations.

As the use of technology and its security has improved over the years, the human aspect of the technology has become very attractive to hackers. Instead of identifying advanced technical exploits, a hacker might be more successful in persuading someone who already has access to a system or technology to give up their credentials. This can typically be done through the hacker pretending to be an authority, and tricking the victim into giving their credentials, or through extortion or blackmail.

It is therefore very important for any individual who has access to systems, technology, or information that is not publicly available, to be aware of such threats, how they work, what they look like, and how to act when such event occurs.

Who am I, and what is the purpose of this study?

My name is Gard Grøttan, and I am conducting this survey in relation to my Master's degree in information security at NTNU Gjøvik.

The purpose of this study is to assess the security awareness of students at NTNU. The results from this study might aid in further developing the security training directed at students at NTNU.

Structure of the questionnaire

The questionnaire takes about 10 minutes to complete, and consists of four main parts:

Part 1: Demographics

Part 1 consists of three questions related to general demographic information. The purpose of this section is to identify whether there are any demographic differences between participants.

Part 2: Knowledge

Part 2 consists of a series of closed questions related to your knowledge of computer use guidelines.

Part 3: Attitude

Part 3 consist of a series of closed questions related to your attitudes towards these use guidelines.

Part 4: Behaviour

Part 4 consists of a series of closed questions related to your behaviour when using your computer at school.

Additional info

You are not obliged to answer any questions in this survey, and if you wish to cancel your submission, you are free to do so at any point in time. If you choose to cancel your submission, your answers will be deleted.

Due to the nature of the data collection method, I will not be able to delete your answers once the questionnaire is submitted, as I will be unable to identify which answers belong to you.

In case of any questions related to the questionnaire, or if you wish to receive a copy of my Master's thesis after it is completed, feel free to send me an e-mail at gardhgr@stud.ntnu.no

Furthermore, this survey has been supervised by Gaute Wangen (gaute.wangen@ntnu.no) and Vasileios Gkioulos (vasileios.gkioulos@ntnu.no).

In order to be eligible for winning a Power gift card (valued at 1000Kr), you have to provide your e-mail address in a separate form that is linked at the end of this survey. Your submitted answers will not be linked with your provided e-mail.

Side 2

Part 1 - Demographics

The following questions are related to general demographic information. The purpose of this section is to identify whether there are any demographic differences between participants.

Gender

- ○ Male
- ○ Female
- ○ Non-binary
- ○ I prefer not to answer

Age

- ○ Below 20
- ○ 20-29
- ○ 30-39
- ○ 40-49
- ○ 50-59
- ○ 60 or above
- ○ I prefer not to answer

Faculty

If you are unsure what faculty you belong to, you can find the list of faculties here:
https://www.ntnu.edu/faculties

Velg ...

Are you a student or an employee at NTNU? *

- ○ I am a student
- ○ I am an employee

I know how to report a security incident at NTNU

- ○ Yes
- ○ No

I know how to report a security discrepancy at NTNU

- ○ Yes
- ○ No

I have completed the "basic information security" training that NTNU provides for all of its students

The course can be found at the following address:
https://studntnu.sharepoint.com/sites/kurs/Sider/Grunnleggende-informasjonssikkerhet.aspx

- ○ Yes
- ○ No

I was aware that NTNU offers a basic information security training course for all students

- ○ Yes
- ○ No

The following statements are about your knowledge of how you should use your computer for school

Password management

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
It is acceptable to use my social media passwords on my school accounts	○	○	○	○	○
I am allowed to share my school account passwords with classmates	○	○	○	○	○
A mixture of letters, numbers, and special characters is necessary for passwords on my school accounts	○	○	○	○	○

E-mail use

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I should be careful to click on any links in e-mails I receive on my school e-mail	○	○	○	○	○
I am allowed to send sensitive personal data or confidential information in e-mails without encrypting the contents first	○	○	○	○	○
If I receive an e-mail with personal sensitive data or confidential information, I should delete the sensitive contents before responding or forwarding the e-mail	○	○	○	○	○

Internet use

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I should be careful downloading files onto my school computer, even if they help me do my schoolwork	○	○	○	○	○
While I am at school, I should not access certain websites	○	○	○	○	○
I should be careful in entering information on websites, even if it helps me do my schoolwork	○	○	○	○	○

Mobile devices

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
The passcode on my phone should not be personal information that is publicly available (e.g. date of birth)	○	○	○	○	○
I should have remote wipe of my phone enabled	○	○	○	○	○
When working on a sensitive document, I must ensure that strangers cannot see my laptop screen	○	○	○	○	○

Information handling

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Sensitive print-outs can be disposed of in the same way as non-sensitive ones	○	○	○	○	○
If I find a USB stick in a public place (classroom, study group room etc.), I should not plug it into my school computer	○	○	○	○	○
I am allowed to leave print-outs containing sensitive information in classrooms/study group rooms overnight	○	○	○	○	○

Incident reporting

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
If I receive a suspicious e-mail on my school account, I must report it	○	○	○	○	○
I must not ignore poor security behaviour by my classmates	○	○	○	○	○
It's optional to report security incidents/security discrepancies	○	○	○	○	○

Computer security

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I must ensure that my school computer and its applications are always updated	○	○	○	○	○
I must have an anti-virus application on my school computer	○	○	○	○	○
I should always use a VPN when I am connected to a guest network outside of NTNU	○	○	○	○	○

The following statements are about your attitude. You've told us about your knowledge of computer use guidelines. Now please tell us what you think about these guidelines.

Password management

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
It is safe to use the same password for social media and school accounts	○	○	○	○	○
It is a bad idea to share my school passwords, even if a classmate asks for it	○	○	○	○	○
It is safe to have a school password with just letters	○	○	○	○	○

E-mail use

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
It is always safe to click on links in e-mails i receive on my school e-mail	○	○	○	○	○
It is risky to send sensitive personal or confidential information in e-mails without encrypting the contents first	○	○	○	○	○
If I receive an e-mail with personal sensitive data or confidential information, nothing bad can happen if I don't delete the sensitive contents before responding or forwarding the e-mail	○	○	○	○	○

Internet use

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
It can be risky to download files on my school computer	○	○	○	○	○
Just because I can access a web-site at school, does not mean that it is safe	○	○	○	○	○
If it helps me do my schoolwork, it does not matter what information I put on a website	○	○	○	○	○

Mobile devices

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
It is risky to have my birth year as my phone's passcode	○	○	○	○	○
It is risky to not have remote wipe enabled on my phone	○	○	○	○	○
It is risky to access documents with sensitive information on a lap-top if strangers can see my screen	○	○	○	○	○

Information handling

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Disposing of sensitive print-outs by putting them in the rubbish bin is safe	○	○	○	○	○
If I find a USB stick in a public place, nothing bad can happen if I put it into my school computer	○	○	○	○	○
It is risky to leave print-outs that contain sensitive information in classrooms/study group rooms overnight	○	○	○	○	○

Incident reporting

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
If I ignore a suspicious e-mail on my school account, nothing bad can happen	○	○	○	○	○
Nothing bad can happen if I ignore poor security behaviour by a class-mate	○	○	○	○	○
It's risky to ignore security inci-dents, even if I think that they are not significant	○	○	○	○	○

Computer security

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
It is risky to postpose pending updates for my school computer and its applications	○	○	○	○	○
It is risky to not have an anti-virus application on my school computer	○	○	○	○	○
Nothing bad can happen if I do not use a VPN when I am connected to a guest network outside of NTNU	○	○	○	○	○

The following statements are about your behaviour. You've told us what you know, and what you think about computer use guidelines. Now please tell us what you do when using a computer for school.

Password management

	Strongly disagree	**Disagree**	Neither agree nor disagree	Agree	Strongly agree
I use a different password for my social media and school accounts	○	○	○	○	○
I share my school password with classmates	○	○	○	○	○
I use a combination of letters, numbers and symbols in my school passwords	○	○	○	○	○

E-mail use

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I do not always click on links in e-mails just because they come from someone I know	○	○	○	○	○
I do not send sensitive personal data or confidential information in e-mail without encrypting the contents first	○	○	○	○	○
If I receive an e-mail with personal sensitive data or confidential information, I delete the sensitive contents before responding or forwarding the e-mail	○	○	○	○	○

Internet use

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I download any files onto my school computer that will help me do my schoolwork	○	○	○	○	○
When accessing the internet at school, I visit any website that I want to	○	○	○	○	○
I assess the safety of websites before entering information	○	○	○	○	○

Mobile devices

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I use my birthday or other publicly available information about myself as a passcode on my phone	○	○	○	○	○
I have remote wipe of my phone enabled	○	○	○	○	○
I check that strangers cannot see my laptop screen if I am working on a sensitive document	○	○	○	○	○

Information handling

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed	○	○	○	○	○
I would not plug a USB stick found in a public place into my school computer	○	○	○	○	○
I leave print-outs that contain sensitive information in classrooms/meeting rooms when I am not there	○	○	○	○	○

Incident reporting

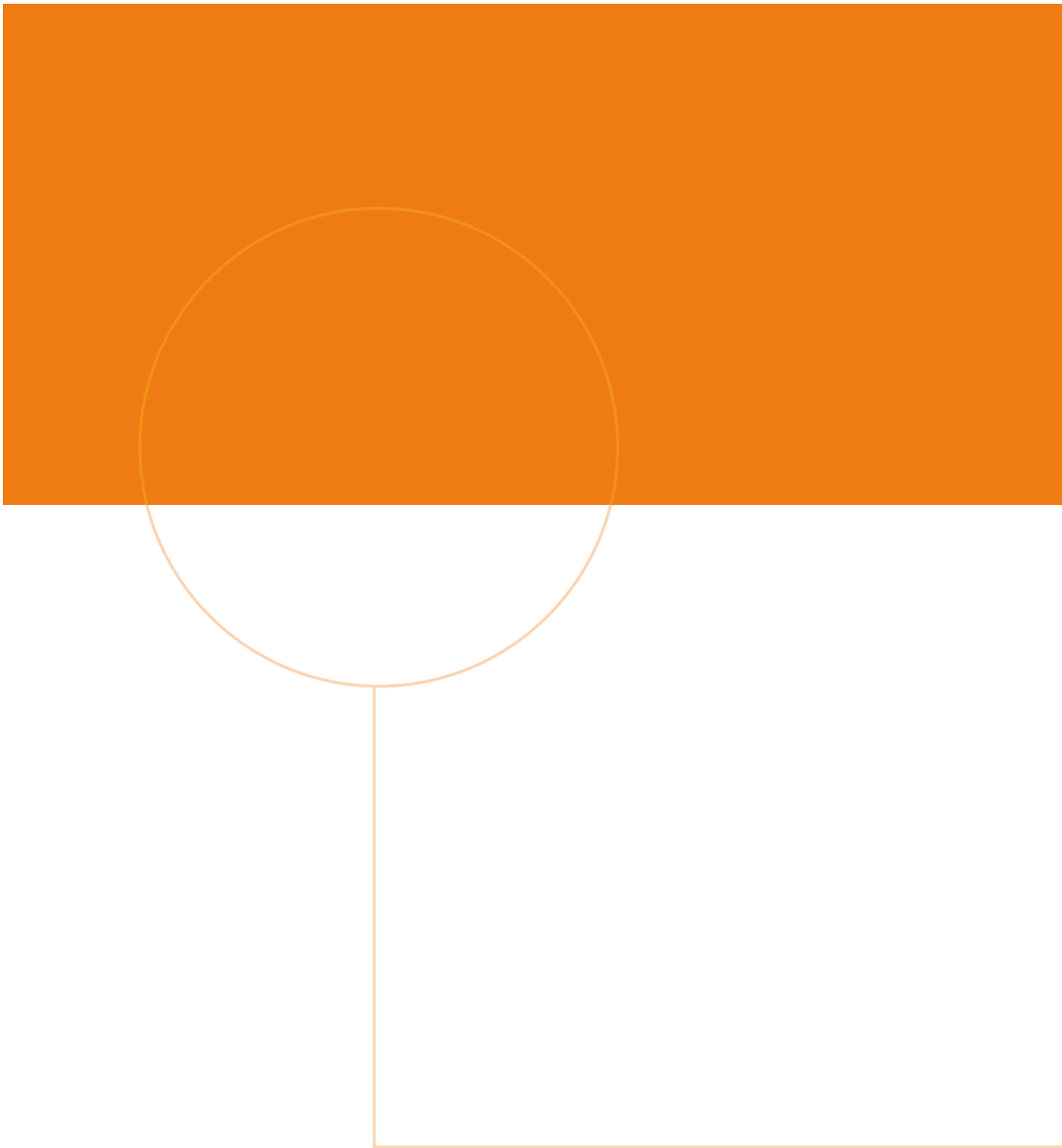
	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
If I receive a suspicious e-mail on my school account, I would ignore it	○	○	○	○	○
If I noticed my classmate ignoring security rules, I would not take any action	○	○	○	○	○
If I noticed a security incident/security discrepancy, I would report it	○	○	○	○	○

Computer security

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I postpone pending updates on my computer and its applications	○	○	○	○	○
I do not have an anti-virus application	○	○	○	○	○
When I am connected to a guest network outside of NTNU, I do not use a VPN	○	○	○	○	○

Sideskift

Do you have any comments or feedback on the questionnaire?



NTNU

Norwegian University of
Science and Technology