
# Enhancing Cybersecurity Awareness for Students at Haaga Helia University of Applied Sciences

Anuj Goyal & Rohan Nahar

Haaga-Helia University of Applied Sciences
Masters in Business Administration
Business Technologies & Leadership Business Transformation
Thesis
2024

## Abstract

**Author(s)**
Anuj Goyal & Rohan Nahar

**Degree**
Master of Business Administration

**Report/thesis title**
Enhancing Cybersecurity Awareness for students at Haaga Helia University of Applied Sciences

**Number of pages and appendix pages**
51

In the current digital era, cybersecurity knowledge is crucial for preserving the confidentiality of personal data and safe online conduct, especially in institutions of higher learning that hold enormous volumes of sensitive data. To uncover knowledge gaps and develop a customised instructional handbook to meet these needs, this research examines the cybersecurity awareness of students at Haaga Helia University of Applied Sciences.

The Social Cognitive Theory (SCT), which prioritises behavioural reinforcement, self-efficacy, and observational learning, served as the theoretical framework for the study. Semi-structured interviews were used as part of a qualitative technique to investigate the attitudes, behaviours, and experiences of students with cybersecurity. Common awareness gaps, misunderstandings, and real-world difficulties encountered by students were identified by the analysis.

This thesis concludes by suggesting that thorough, approachable instructional materials, like the created handbook, can be extremely helpful in closing the knowledge gap in cybersecurity among students. To encourage improved cybersecurity practices and provide a safer online environment for all students, it is advised that educational institutions include this handbook in their resources.

**Keywords**

Cybersecurity, Student Awareness, Cyberthreats, Digital Safety, Online Privacy, Handbook Development

## Table of contents

# 1 Introduction

Due to the sensitivity of student and faculty data, higher educational institutions are facing unique challenges regarding cybersecurity. As a result, it has become an essential concern for institutions across the globe. The development of digital technologies has transformed various sectors, notably education (OECD 2018,15-16). Along with enabling knowledge access and dissemination, these advancements have manifested an intricate web of cybersecurity concerns (European Union Agency for Cybersecurity 2022, 6-7). Higher learning institutions that house confidential data and intellectual property are particularly vulnerable to cyberattacks (National Institute of Standards and Technology 2021, 12-15).

Cybersecurity breaches can lead to serious consequences for higher education institutions, including monetary losses, harm to their reputation, and disruption of academic endeavours (Bhattacherjee 2016). Universities have a huge obligation to protect sensitive data from unauthorised access because they are the stewards of valuable student data (General Data Protection Regulation 2016, 32). However, the effectiveness of these security measures depends on a foundation based on a strong understanding and awareness of cybersecurity among all parties connected to each institution, including students, faculty, and staff.

These technologies, which range from digital research repositories to online learning platforms, have surely improved accessibility and efficiency in Finland's academic environment (NCSC-FI 2023, 15-25). But these developments also bring an increasingly dangerous threat scenario in the form of cybersecurity threats. Cyberattacks target academic institutions like Haaga Helia University of Applied Sciences because they are the guardians of enormous volumes of sensitive data, such as research findings, student information, and intellectual property. Successful breaches have repercussions beyond simple data loss; they may jeopardise the quality of scholarly research, undermine institutional confidence, and violate staff and student privacy rights (Council of Europe 2020).

Despite the growing awareness of cyber dangers, students' comprehension of cybersecurity is often lacking according to research (Li et al. 2019, 105-110). This lack of awareness may lead to irresponsible online behaviour and compromise institutional security by causing data breaches (Sweeney 2018, 125). Therefore, to reduce these hazards, cybersecurity education must be expanded for kids.

## 1.1 Background

Higher education institutions (HEIs) are increasingly vulnerable to cyberattacks, posing a critical concern for cybersecurity. As HEIs contains valuable and confidential student data, research

outcomes, as well as intellectual property - they have become lucrative targets of malicious attackers (Sweeney 2018, 125). If successful in their attacks on these websites or networks, the consequences can be severe with potential implications ranging from high financial losses to reputational damage and disruptions within academic activities (Bhattacherjee 2016).

HEIs have been identified as vulnerable to cyber threats through consistent research (European Union Agency for Cybersecurity 2022, 6-7). These risks are amplified due to the decentralised structure of higher education and reliance on third-party service providers. Moreover, the increasing use of technology in teaching and research further increases this vulnerability (National Institute of Standards and Technology 2021, 12-15).

The awareness and knowledge of an institution's members are essential components for its cybersecurity posture. Despite being perceived as digital natives, students' comprehension of cybersecurity concepts and practices is typically deficient (Li et al. 2019, 105-110). Studies have indicated a connection between low cybersecurity consciousness among students and perilous online behaviours (Sweeney 2018, 130-141), which may result in negative outcomes for both individuals and institutions alike.

Former research has investigated diverse elements that impact the cybersecurity awareness of students, such as age, gender, educational history, and exposure to instruction on cybersecurity (Chen & Huang 2017, 50-60). Nevertheless, more examination is necessary into higher education institutions’ specific settings and the exceptional obstacles experienced by learners in this milieu.

To acknowledge the significance of cybersecurity awareness, several Higher Educational Institutions (HEIs) have introduced education and training programs to tackle this issue. These projects differ in size as well as mode of delivery; some present online modules that are mandatory, while others focus on specific cybersecurity courses. Nonetheless, their effectiveness in terms of improving students' comprehension and conduct is often doubted by experts (Huang & Chen 2018, 110-120).

Several obstacles in providing students with practical cybersecurity education have been identified through research, and these include the necessity for stimulating content, hands-on learning opportunities, and continued reinforcement of knowledge (Sweeney 2018, 130-141). Creative techniques and instructional methodologies must be employed to tackle these hurdles effectively.

## 1.2 Objectives

The main objective of this study is to improve the understanding and education regarding cybersecurity among students at Haaga Helia University of Applied Sciences. To attain this goal, the research will:

Evaluate students' present level of cybersecurity knowledge and awareness; and find out how they view cyber threats, vulnerabilities, and optimal cybersecurity practices.

The main objective is to pinpoint the unique hurdles and advantages linked with cybersecurity at a student level. This undertaking entails examining various factors that impact students' mindsets and actions towards online security, in addition to uncovering any inadequacies within current educational curricula pertaining to cyber safety.

## 1.3 Research problems and questions

To determine the students' baseline awareness, it is crucial to assess their knowledge of cybersecurity related practices at Haaga Helia University. This includes evaluating students' understanding of basic ideas like malware, phishing, and social engineering as well as looking at security best practices including password management, data protection, and online privacy. By measuring students' current knowledge, it is possible to determine where instructional efforts should be focused, leading to a better-equipped student body in terms of cybersecurity awareness.

To customise successful educational interventions, it is crucial to identify significant areas that need improvement in students' knowledge of cybersecurity. This requires discovering precise areas where students lack understanding and misunderstandings. By reviewing the outcomes from evaluations on cybersecurity, we can figure out which topics necessitate more focus or emphasis. For instance, if data collection shows inefficiencies concerning password management techniques or data protection significance comprehension, these domains should receive immediate attention during educational programs.

To create a cybersecurity handbook, the research questions crucial for reaching the objectives of the development task are as follows:

What is the current level of knowledge about cybersecurity among students at Haaga Helia University of Applied Sciences?

What are the key areas of improvement needed to enhance cybersecurity knowledge among students?

What content should be included in a cybersecurity handbook tailored for students at Haaga Helia University of Applied Sciences?

### 1.4 Case Institution: Haaga Helia University of Applied Sciences

The dynamic Haaga Helia University of Applied Sciences offers a broad range of courses in business, computer technology, hospitality, and communication. Its main campus is located in Helsinki, Finland. Renowned for its emphasis on experiential learning and industry engagement, Haaga Helia prepares students for success in the workplace in a global context (Haaga Helia 2023). Focusing on innovation, digital transformation, and lifelong learning, the university serves a diverse student body over seven campuses.

### 1.5 Existing Cybersecurity Practices at Haaga Helia

Haaga Helia has taken several steps to protect its administrative and academic functions from online attacks. These consist of:

- **Technical Infrastructure:** The institution utilises firewalls, secure servers, and antivirus software to protect its network and data from malicious intruders. Regular vulnerability assessments and system updates are conducted to strengthen protections (NIST 2021, 15-25; ENISA 2022, 30-40).
- **Policy Framework**: To ensure adherence to laws such as the General Data Protection Regulation (GDPR), policies about data protection and permissible IT use are in place (GDPR 2016, 10-20). These guidelines specify duties, obligations, and proper conduct for both employees and students.
- **Awareness Initiatives:** Targeting typical dangers like phishing and password protection, periodic workshops and awareness campaigns teach the fundamentals of cybersecurity (Li et al. 2019, 45-60). These initiatives do not yet, however, form part of a formal curriculum for students.
- **Online Learning and Resources:** Students engage with digital repositories and online platforms such as Microsoft Teams, Moodle, and others that are protected by authentication methods (Moodle 2023, 10-20). Human factors—like weak passwords or phishing susceptibility—remain weaknesses despite these precautions (Sweeney 2018, 130-141).

### 1.6 Structure of thesis

Chapter One: The introduction chapter provides essential information that serves as the basis for cybersecurity research. By highlighting the necessity for Haaga-Helia students to increase their awareness of cybersecurity, the problem statement highlights an existing gap. This chapter ends with specific research questions and objectives that describe how the study's value meets the previously defined needs.

Chapter Two: The theoretical framework chapter outlines the theoretical underpinnings of the research project and develops a conceptual framework for assessing cybersecurity awareness for the case company, drawing on pertinent literature. It clarifies how the theoretical foundations direct the research and influence how the findings are interpreted.

Chapter Three: The methodology chapter outlines the research strategy used to determine the degree of cybersecurity awareness among Haaga-Helia pupils. In addition to discussing data collecting procedures (focus group interviews), this section goes into detail about methods for drawing important conclusions from collected data while conducting analysis.

Chapter Four: This development task's chapter focuses on developing a brief handbook proposal that uses study findings to raise cybersecurity awareness among Haaga-Helia pupils. The goal of the development process is to teach important cybersecurity concepts while considering knowledge gaps and student needs easily and actively. This chapter provides recommendations for Haaga-Helia University of Applied Sciences to establish and grow cybersecurity education programs following an analysis of the research findings and the creation of a brief handbook. The suggestions include integrating cybersecurity concepts into current courses, making effective use of available resources, and encouraging an organization-wide cyberdefense culture.

Chapter Five: The discussion chapter provides more insight into the significance and ramifications of the research findings. The chapter highlights how these findings enhance understanding while establishing connections between them and the current theoretical framework. This section highlights the significance of the study's findings by comparing them to previous research. It also assesses any methodological difficulties in carrying out such a study and suggests solutions for future research aiming to progress the field.

Chapter Six: The study's last chapter highlights how this analysis enhances cybersecurity education, specifically at Haaga-Helia University while summarizing the key findings and restating the study's objectives. By emphasizing the useful applications of these discoveries and outlining avenues for additional research in subsequent studies, the conclusion makes an impression.

## 1.7 Scope

Students enrolled at Haaga Helia University of Applied Sciences cam-puses are the study's primary focus. Students' cybersecurity awareness, knowledge, and behaviours were investigated using a qualitative research methodology. Key areas of scope included:

Evaluating students' understanding of common cyber threats (e.g., phishing, malware, social engineering).

Examining the existing cybersecurity education initiatives and awareness within the university by interviewing students from different courses.

Developing a handbook for enhancing cybersecurity education among students to safeguard academic and personal data.

By focusing on these areas, the research aims to provide a comprehensive understanding of the cybersecurity landscape among Haaga Helia students and to offer actionable recommendations for improvement.

## 1.8 Delimitations

Although this thesis offers insightful information about Haaga Helia University of Applied Sciences students' cybersecurity knowledge and education, several boundaries were set to keep the study feasible and focused. These consist of:

**Geographic Focus:** Students from other universities are not included in the study; it is limited to Haaga Helia University of Applied Sciences. This could restrict the findings' applicability to students in various learning contexts or geographic areas.

**Participant Scope:** Faculty, administrative personnel, and outside stakeholders who are also vital to the institution's cybersecurity environment are not included in the study; instead, its main focus is on students.

**Technical Scope:** The research doesn't go into detail on the university's cybersecurity procedures, tools, or technical infrastructure. Instead, it emphasises the behaviours, awareness, and students' knowledge.

# 2 Theoretical Framework

In today's innovative technological world, students are using technology increasingly for social, intellectual, and personal reasons; and educational institutions are essential in helping students become conscious of cybersecurity. According to research, students are especially susceptible to cyberthreats because of their extensive online usage and frequently inadequate understanding of cybersecurity (University of Jyväskylä 2016, 30-40).

This section provides an overview of the prior research conducted in assessing the awareness level of individuals in cybersecurity. In comprehensive education, it is essential to equip young individuals with the necessary skills for the cyber domain, enhance their understanding of cybersecurity threats, and enable them to protect themselves effectively. According to a study (University of Jyväskylä 2016, 30-40), there is a recommendation to incorporate cybersecurity education across various educational levels. As students progress to upper-secondary and vocational education levels, these competencies are more refined, laying the groundwork for specialized expertise in higher education. Vocational education can offer cybersecurity education and training that provide foundational professional skills and qualifications required in the workplace. In recent years, the rapid advancement and widespread adoption of newer digital technologies have significantly transformed various aspects of academic institutions in Finland. This digital adoption has reshaped how students learn, engage, and deliver their content, and how institutions operate, manage, and do other academic activities.

To support online learning and content delivery, Finnish academic institutions have embraced digital learning platforms like Moodle and its open-source substitutes (NCSC-FI 2023, 15-25). These would improve flexibility and enable creative teaching approaches in the classroom by enabling students to freely access learning resources, turn in assignments, take part in online conversations, and receive feedback from teachers. There is no denying that these technologies have improved accessibility and efficiency in Finland's educational system as well (NCSC-FI 2023, 15-25), but these developments are accompanied by a growing threat landscape of cybersecurity threats.

## 2.1 Importance of Cybersecurity Education among Students

The necessity of including cybersecurity education in curricula at all levels has been a famous subject of research. For example, a study by Finland's National Cyber Security Centre (NCSC-FI, 2023,15-25) discovered that students are exposed to cybersecurity vulnerabilities when they use digital platforms like Moodle. Academic institutions must tutor students in cyber hygiene and safe online conduct because of the growing use of these platforms.

## 2.2 Key concepts and theories in cybersecurity in academics

A few core ideas and approaches that address how people perceive, learn, and sustain secure online activities are highlighted in academic research on cybersecurity education for students. The Social Cognitive Theory (SCT) (Bandura 1986, 50-70) is pertinent to comprehending students' cybersecurity habits since it highlights the importance of reinforcement, self-efficacy, and observational learning in behaviour adoption. The Protection Motivation Theory (PMT) (Rogers 1983, 153-170) is another well-known concept. It asserts that people are motivated to implement security measures by their perception of the threat's seriousness and their own ability to stop cyberattacks. Also commonly used is the Technology Acceptance Model (TAM) (Davis 1989, 319-340), which examines how students' adoption of protective behaviours may be influenced by their perceptions of the cybersecurity technologies' utility and ease of use.

Furthermore, the Theory of Planned Behaviour (TPB) (Ajzen 1991, 181-203) describes how students' intentions to practice cybersecurity are influenced by attitudes, social norms, and perceived behavioural control. Key ideas include resilience and cyber hygiene, which promote consistent, preventative actions like two-factor authentication and strong passwords. Self-Determination Theory (SDT) (Deci & Ryan 2000, 68-92) investigates the underlying motivations for these safe habits.

Because of its strong approach to comprehending learning in social circumstances, we decided to use Social Cognitive Theory (SCT) as the guiding framework for our thesis. The study of cybersecurity behaviours in an academic context, where students frequently pick up knowledge from peers and institutional policies, is a good fit for SCT's emphasis on observational learning and self-regulation. Because cybersecurity requires students to feel both competent in defending themselves and motivated to sustain secure practices, the theory's emphasis on self-efficacy and the reinforcement of positive behaviours is particularly pertinent. To provide a thorough foundation for assessing and improving Haaga Helia University students' security practices, we intend to use SCT to examine the relationships between individual behaviours, contextual conditions, and social impacts on cybersecurity awareness.

## 2.3 Importance of theoretical models in understanding awareness and behaviour

According to Bandura (1986), these models are essential for comprehending the awareness and behaviour roles that individual and environmental factors play in cognitive, vicarious, self-regulatory, and self-reflective processes related to human adaptation and transformation. Understanding how consciousness is formed, how it manifests as behaviour, and how confident people are in using that knowledge, as well as the social and environmental signals that support behaviours, is made possible by the Social Cognitive Theory (Der. Da 2002, 45-70). University authorities across

the world can seek to improve their students' emotional states, correct their flawed self-beliefs and thought patterns (personal factors), enhance their academic abilities and self-regulatory behaviours (behaviours), and change their study plan structures or cyber practices that could jeopardize their success (environmental factors) by employing social cognitive theory (Schunk, D.H. 2012, 139-160).

## 2.4 Social Cognitive Theory (SCT)

This master's thesis research's real-world concepts and facts served as the basis for the decision to use the Social Cognitive Theory (SCT), which gives us a thorough framework for comprehending how Haaga Helia students can apply what they have learnt to become more cyber-aware and develop realistic concepts. To explore the broad notion of cybersecurity and how pupils learn it, SCT places a strong emphasis on the dynamic interaction between personal characteristics, behaviours, and the environment. The theory is composed of many fundamental components that, when combined, help to better understand students' existing awareness levels, and provide a basis for creating interventions that will enhance cybersecurity education in the real world (Zimmerman 2000, 57-80). Understanding how student communities use control and reinforcement to create goal-directed behaviour that can build confidence in adopting safe online practices is the aim of selecting the Social Cognitive Theory.

In the 1980s, Albert Bandura developed a psychological framework known as the Social Cognitive Theory (SCT) to explain how people learn and regulate social behaviours through the dynamic interaction of behavioural, personal, and environmental elements (Bandura 2001, 10). People actively modify their behaviour by watching others, copying their activities, and thinking about the repercussions of their actions, according to SCT theory. It highlights that people are actively involved in their growth and that they have the power to influence events. SCT, which was developed from Bandura's earlier work on Social Learning Theory in the 1960s, considers an individual's prior experiences, which influence whether they would take behavioural action. SCT is currently especially important in investigating how students gain awareness and modify their internet behaviour in a variety of situations, such as educational, personnel, and organizational settings because cognitive elements have been incorporated into behavioural theories (D.F. Pajares 2010, 56-78). This strengthens how behavioural, environmental, and personal elements interact.

## 2.5 Key Components of SCT

### 2.5.1 Reciprocal Determinism

This is the main concept of Social Cognitive Theory that refers to the dynamic and reciprocal interaction of individuals, how they think and feel, their environment, and the behaviour itself stimuli to

achieve a goal. These are interdependent and mutually influence one another, offering a holistic view of behaviour change, as interactions between what individuals think, how they act, and the environment they operate within.

- Individual**:** It refers to personal internal characteristics of an individual, including their thoughts, beliefs, attitudes, and emotions, which play a crucial role in determining how confident a student feels about performing a cyber behaviour.
- Environmental: It encompasses all external, social, and physical surroundings that can affect an individual's behaviour. It could be both social influences such as peer behaviour, societal norms, and structural factors such as the resources availability or policies.
- Behavioural**:** It refers to the actions an individual takes, which are influenced by personal factors and environmental conditions (Cherry, K. 2023, 45-60). Behaviour also impacts their thoughts and the environment they operate within; however, people learn from the consequences of their behaviour, further affecting the environment in which they live (Bandura, 1989, 36-50).

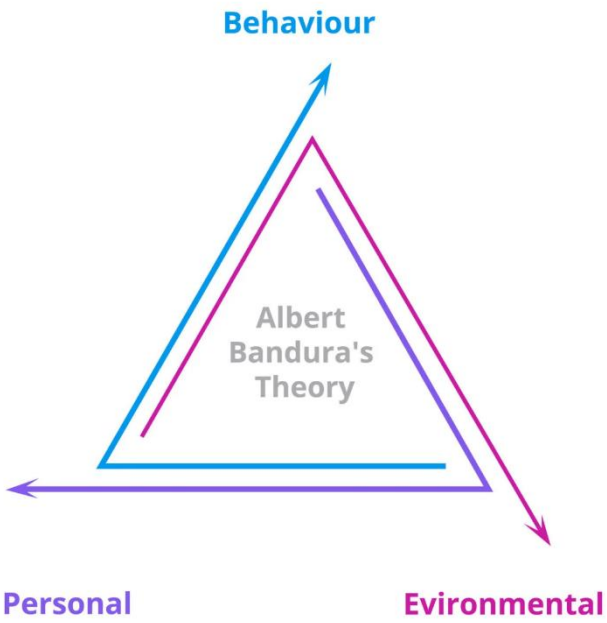



**Figure 1**: Nickerson, C. (2024). Albert Bandura's Social Cognitive Theory. Simply Psychology. URL: https://www.simplypsychology.org/social-cognitive-theory.html.

### 2.5.2 Behavioural Capability

It refers to a person's real capacity to carry out an action using the necessary knowledge & skills required so that a person needs to understand what to do and how to do it to carry out a behaviour successfully. Individuals get knowledge from the results of their actions, which also have an impact on their surroundings.

- Knowledge**:** Knowledge forms the foundation of behavioural capability, as individuals must know what to do before they can act. A person's behavioural capability hinges on both their cognitive understanding and their practical competence (Nickerson, C., 2024, 110) to understand the steps, processes, or actions required to engage in a particular behaviour.
- Skills**:** To promote a desired behaviour, skills are the practical abilities or competencies that allow a person to perform the behaviour successfully. Even if an individual knows the importance of a behaviour, they also need the skills to execute it properly.

### 2.5.3 Observational Learning

It also known as modelling, is a key component of Social Cognitive Theory (SCT) in which individuals acquire new behaviours by observing others (Stone, S. 2017, 45-65). People can learn by watching the actions of others and the consequences that follow those actions. Albert Bandura emphasized four conditions were necessary in observing and modelling behaviour: attention, retention, reproduction, and motivation. Albert Bandura demonstrated the power of observational learning in his famous Bobo doll experiment, where children who observed adults behaving aggressively toward a Bobo doll were more likely to replicate that behaviour themselves (Miller, S Lang, D. 2022, 100).

- Attention**:** An observer must pay attention to the person performing the behaviour. Factors such as the model's attractiveness, status, similarity to the observer, or perceived competence can affect how much attention is paid to the behaviour.
- Retention**:** The behaviour must be remembered to be replicated. Retention may involve encoding the observed behaviour into memory so it can be retrieved and used later.

### 2.5.4 Self-efficacy

Self-efficacy is a key element of Social Cognitive Theory because it affects the motivation, learning (Pajares, 1996, 2006; Schunk, 1995, 2003) and belief in their ability to perform behaviours. Self-efficacy is unique to SCT although other theories have also been added later, such as the Theory of Planned Behaviour. Four main sources of information that create students' self-efficacy: enactive mastery experiences, vicarious (observational) experiences, social persuasions, and physiological and psychological states (Bandura 1997, 80-95).

### 2.5.5 Expectations

Outcome expectations determine whether people believe that behaviour will lead to desired results. It plays a critical role in influencing a person's decisions, behaviours, and motivation. According to Albert Bandura, individuals who engage in behaviours not just based on immediate rewards or punishments, but also on what they expect will happen because of their actions. (Lee, Muñoz, M. 2015, 40-60).

- Influence on Motivation: It directly affects a person's motivation to engage in a particular behaviour, often people are more motivated to act if they expect positive outcomes from their actions.
- Behavioural Choices: When people anticipate positive outcomes, they are more likely to engage, while they may avoid behaviours that they expect will have negative consequences.
- Persistence: It refers to how people persist in the face of obstacles. When individuals expect that their efforts will eventually lead to success, then they are more likely to keep going.
- Emotional Responses: Positive expectations can lead to feelings of excitement, confidence, and hope, while negative expectations can result in anxiety, fear, or frustration.

## 2.6 Application of SCT to Cybersecurity Awareness

Social Cognitive Theory is a valuable framework for understanding how students become aware of and learn cybersecurity practices before any threat or risk. We understand cybersecurity is a broad concept having multiple complexities & making it difficult for each student to understand but we can find a common ground where we involve behaviours that protect students and organizations from newer digital threats. We analyse & explain how people adopt these behaviour practices through key concepts of observational learning, self-efficacy, reinforcement, and outcome expectations in a Social Cognitive Theory (Tamrin, Hamid, S. 2021, 45-65). The core principle of SCT is that people learn by observing others. In the context of cybersecurity, this means individuals can learn safe online behaviours by observing others, whether it be colleagues, friends or staff members to practice safe cybersecurity habits such as regularly updating software, using strong passwords, and avoiding suspicious links (TSC, The Bandura Effect, 2023, 20-40). The IT security team of an institution might demonstrate the correct way to identify potential threats beforehand during the beginning of their academic session.

To increase cybersecurity awareness and behaviours, it is also essential to boost students' confidence that they can recognize and handle potential threats by enrolling themselves in training programs or cybersecurity awareness campaigns organized by institutions which can help students feel more competent & comfortable in protecting themselves from cyber threats. As they

experience success with these tasks, their belief in their ability to protect themselves from more complex cyber threats will grow. As they experience success with these tasks, their belief in their ability to protect themselves from more complex cyber threats will create an environment from more complex cyber threats in the digital world. It has been observed in previous research that individuals who regularly update their software to protect their systems from malware are more likely to keep their applications up to date. For instance, seeing a student recognized for completing mandatory cybersecurity training may motivate others to reinforce safe practices by offering incentives, rewards, or recognition. This interaction between personal awareness, behaviour, and institutional emphasis on security illustrates the key concept of reciprocal Social Cognitive Theory. By organizing awareness campaigns, students who see their peers receiving positive recognition may be more likely to engage others to do the same.

## 2.7 Relationship of cybersecurity awareness with Social Cognitive Theory SCT components

- **Behavioural Capability:** Cybersecurity awareness through the SCT key factor of behavioural capability focuses on the knowledge & skills of students to know cybersecurity principles and understand their capability to apply these skills effectively. The key methods, such as quizzes, practical exercises, phishing simulations, and real-world scenario analyses, are crucial components for understanding critical topics like Threats (phishing, malware, ransomware, and social engineering), Password Security (length, complexity, avoiding common words), Privacy, Safe Internet Practices or Protection (avoiding suspicious websites, recognizing unsecured connections and encrypted communications e.g., HTTPS for sensitive information) where they may need additional training (Six, H., 2024, 50-70). The equal importance of their behavioural capability to apply their knowledge & skills to evaluate whether students need to take appropriate actions when facing cyber threats in their academic journey.

- **Observational Learning:** Social Cognitive Theory (SCT), particularly through the lens of observational learning for students, provides a strong framework for understanding how individuals develop awareness and learn key cybersecurity practices through Observational, or say learning by watching others. It is highly relevant how students can acquire new behaviours by observing the actions of other peers and friends, and by examining the influence of behaviour, observing their efforts (like using strong passwords), faculty teaching (access to critical systems), and online resources (password management or anti-virus software). In past, research has also shown that when individuals expect that cybersecurity practices will lead to positive outcomes (SoSafe 2023, 3-15), such as protecting personal

data, avoiding cyberattacks, or maintaining access to critical systems—they are more likely to be motivated to follow through.

- **Self-efficacy:** An individual's belief in their ability to perform the behaviour they have observed. It is significantly important for students to assess their confidence in applying higher self-efficacy behaviour that leads to a greater likelihood of attempting to reproduce the safe habits. Successful imitation of a behaviour strengthens self-efficacy, leading to adopting new behaviours in the future. In this model behaviours like problem-solving, peer learning, discipline, social interaction, observing or learning cognitive social skills are common task-specific examples, meaning a person may have high self-efficacy in one area, and seek to achieve their goals.

- **Reinforcements and Expectations:** The relationship between reinforcements and expectations work together to guide individuals, behaviour, and the environment. Observing the outcomes of behaviours (vicarious reinforcement) shapes outcome expectations, and the individual's self-efficacy (efficacy expectations), factors influencing motivation to adopt cybersecurity behaviours. Reinforcements can be external (coming from outside sources, like praise or punishment) or internal (self-satisfaction from achieving a goal or performing well). In a research, data shows those universities that run an awareness campaign among their students, are more capable of implementing safe practices effectively and they are more likely to consistently engage others in safe & secure behavioural practices. (Chaudhary, S. & Gkioulos, S. 2022, 45-68).

In this chapter, we have looked at a few important ideas and theories that are essential to comprehending cybersecurity education, especially when it comes to pupils. As students are exposed to possible cyberthreats through digital platforms and online interactions, the significance of cybersecurity education is becoming more widely acknowledged in educational institutions (NCSC-FI, 2023,15-25). A variety of theoretical frameworks, including the Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), Technology Acceptance Model (TAM), and Social Cognitive Theory (SCT), offer important insights into how students view, embrace, and uphold safe online conduct. Particularly noteworthy is SCT's focus on reinforcement, self-efficacy, and observational learning as factors influencing students' cybersecurity behaviours. By utilising these theories, we can comprehend how students learn about cybersecurity, how they are inspired to use it, and how their social and institutional environments influence their awareness and actions.

SCT is especially well-suited to comprehending how individuals in academic contexts adopt cybersecurity practices because of its emphasis on the dynamic interplay between psychological, behavioural, and environmental elements. The emphasis on self-regulation and observational learning in this theory is consistent with how pupils pick up knowledge from their peers and institutional regulations. Additionally, the integration of self-efficacy and reinforcement processes in SCT offers a strong basis for investigating how students' motivation and self-assurance impact their cybersecurity practices.

# 3 Methodology

The purpose of this study was to find out how much the students at Haaga Helia University of Applied Sciences knew about cybersecurity and to develop a guide that would help raise their understanding of the topic. This methodology allowed for an examination of students' knowledge, attitudes, behaviours, and experiences linked to cybersecurity. The kind of research technique known as action research involves first identifying an issue and then taking steps to resolve it. It involves a cycle of planning, carrying out, observing, and reflecting. Action research is distinguished by its focus on collaborative efforts, contextuality, and practical results (Kemmis & McTaggart 2018, 25–45). Action research and other qualitative research methods are the best research strategies to support the content of the study given its goal. The study's target, Haaga Helia University of Applied Sciences in Finland, was chosen because of its wide range of academic programs and heavy reliance on digital tools and platforms for administration and learning. Given that it is a higher education institution and integrates digital technologies into both academic and operational activities, it offers the perfect setting for investigating cybersecurity awareness among students.

The institution is a good place to assess cybersecurity awareness and practices among students with different technological backgrounds because it serves a large student body from a variety of academic fields, including commerce, IT, and tourism. Despite not having formally commissioned this study, Haaga Helia's student demographics and dependence on digital platforms offer a great chance to investigate and resolve cybersecurity issues in higher education.

## 3.1 Research Methods

Action research is a useful approach for solving practical issues and encouraging ongoing development. Action research is based on circumstances and surroundings. Action research has the potential to be beneficial and results in major advancements (Stringer 2023, 60-80), but it can also be laborious and have limitations regarding generalizability (Yin 2025, 120-140).

As per the famous book on qualitative research by Creswell & Poth (2018, 150-180), the following steps are commonly included in the action research process:

- Problem identification is the process of determining which issue or problem requires attention.
- Planning: Creating a strategy that includes goals, objectives, and tactics to address the issue.
- Acting: Putting the planned steps into action and gathering information.
- Observing: Examining and considering the outcomes of the deeds.
- Reflecting: Assessing how well the actions worked and modifying them, as necessary.


Figure 2: Action Research Process (Lewin 1946)

The concept of Action Research was introduced by Kurt Lewin in the 1940s, who viewed it as applying scientific principles to solve social issues (Lewin 1946, 2). Lewin's initial work focused on changing social behaviour through cycles of planning, acting, and evaluating outcomes. Over time, Action Research has evolved to be applied across various fields, including education, healthcare, business, and community development. Its emphasis on involving those affected by the issue in the research process makes it particularly suitable for environments where change is needed. Since changing attitudes, beliefs, and practices require knowledge of attitudes and practices, action research is particularly pertinent to behavioural and educational studies.

Action Research is widely applied in fields that require continuous improvement and adaptation. In education, for instance, teachers often use Action Research to enhance teaching methods or student learning outcomes (Kemmis, McTaggart & Nixon 2014, 45-80). In business, Action Research helps managers and employees collaboratively address workplace challenges and improve processes (Sagor 2011, 35-60). Its focus on practical problem-solving and its participatory nature make it highly adaptable across various fields (Reason & Bradbury 2008, 20-40).

Action research has a few benefits, especially when change is intended. Its participatory character, which directly incorporates individuals impacted by the problem in formulating solutions, is one of its main advantages. This guarantees that the interventions are pertinent and customized to meet the requirements of the group or institution (Reason & Bradbury 2008, 25-50). Furthermore, action research is adaptive and fluid, enabling changes to be made at any point in the process in response to immediate feedback and introspection (Coghlan & Brannick 2014, 25-50). The method's cyclical structure promotes continual progress, which makes it an effective tool for developing capacity and tackling long-term problems.

For this reason, action research is an effective method for bridging theory and practice, as it emphasizes collaboration, flexibility, and solving real-world issues. It is a helpful tactic for academics hoping to have an impact on their profession (Herr & Anderson 2015, 10-40). Action research involves participants in the research process and provides practical solutions, empowering individuals to take responsibility for the changes they wish to see in the world. However, the method's effectiveness depends on thorough planning, moral consideration, and ongoing reflection to ensure

that the desired outcomes are achieved in a meaningful and long-lasting way (Reason & Bradbury 2008, 25-50).

### 3.2 Research Strategy

A research strategy is the plan or approach that guides the way a research study is conducted. It outlines how the researcher intends to answer the research questions or achieve the objectives by selecting the appropriate methods, procedures, and techniques for data collection and analysis. The research strategy ensures that the research is structured, systematic, and aligned with the goals of the study. It also determines whether the study will follow a qualitative, quantitative, or mixed-methods approach, depending on the nature of the research problem (Creswell & Creswell 2018, 3-15).

For this thesis conducted in Autumn 2024, a qualitative research approach is used since the primary objective of the research strategy is to examine and understand students' awareness around cybersecurity. Focus groups acted as an essential part of this strategy since they allowed for in-depth discussions on the challenges, experiences, and awareness of the students. This qualitative approach is crucial for gaining insights that cannot be gained from quantitative surveys by itself. Through interactive group conversations and the research's aim to uncover intricacies in students' understanding of cybersecurity, the development of a handbook to increase cybersecurity awareness was made possible.

The creation of a cybersecurity awareness handbook based on the information from the focus group interviews was one of the main results of this study. For Haaga Helia students, this handbook will be a useful tool since it offers concise instructions on important cybersecurity topics like password management, phishing, and safe usage of public networks. The handbook will be immediately applicable to the daily lives of the students because it is specifically tailored to address the needs and concerns that were highlighted in the focus groups (Sagor 2011, 30-50). The action component of action research, which produces useful results intended to address real-world issues, is best illustrated by this development stage (Kemmis, McTaggart & Nixon 2014, 45-60).

### 3.3 Practical Significance of the Initial Issue

Due to the growing threats posed by cyberattacks in today's digital ecosystem, the original problem—in this example, the lack of cybersecurity awareness among students at Haaga Helia—has practical relevance. Students who use online learning and communication platforms run the danger of falling victim to identity theft, phishing frauds, and data breaches, among other cybersecurity hazards. Comprehending the ramifications of these hazards is essential for safeguarding students' confidential information as well as maintaining the credibility of the educational establishment

(Hadnagy 2018). By tackling this problem, the study hopes to equip kids with the skills necessary to safely traverse digital places and foster a safer online environment for them. A useful remedy, like a short cybersecurity handbook, can address this urgent problem eventually.

### 3.4 Acquiring Knowledge about the Subject

A comprehensive understanding of the subject matter is essential for the accomplishment of any investigative project. Since we both are from IT backgrounds, together with peer interactions and prior knowledge, we acquired further knowledge about the subject. A thorough literature assessment enables academics to pinpoint knowledge gaps and frameworks that can guide the creation of instructional materials (Blakley et al. 2001, 15-40). In addition, conducting focus group interviews with students directly offered insights into their current beliefs, experiences, and actions related to cybersecurity. This dual method, which highlighted both theoretical perspectives and practical applications, produced a well-rounded grasp of the subject by combining a literature review with direct interactions.

### 3.5 Designing and Suggestions on the Handbook

A crucial step in the study process was designing the handbook, which turned the knowledge gathered from the literature review and focus groups into a useful tool for students. The handbook is designed to be specifically customized to the needs of the Haaga Helia student body by addressing the top cybersecurity concerns that were brought up during the focus group interviews (see appendix 2 for the handbook). This required breaking up the content into manageable, easily navigable parts covering important subjects including phishing attempt detection, password management, and secure public Wi-Fi usage guidelines (Chabrow 2014, 50-80).

### 3.6 Data Collection

#### 3.6.1 Sampling

Students from a range of courses at Haaga Helia University of Applied Sciences participated in the focus group interviews. For each focus group, 4 to 5 students were chosen from various courses using purposive sampling. Purposive sampling, a non-probability sampling technique used exclusively in qualitative research, entails deliberately choosing individuals with traits to increase sample diversity and data richness (Hennink and Associates 2020, 330). A wider range of viewpoints on cybersecurity practices and risks were made possible by this strategy, which guaranteed a diversified representation of students with differing degrees of cybersecurity awareness. To comprehend how students from various academic disciplines see cybersecurity and related practices, the sampling approach was essential. Five focus groups were held, each with 4-6 students from bachelor's

and master's degree programs, with a total of 21 participants. This arrangement promoted lively conversations and made sure that a variety of perspectives were recorded.

### 3.6.2 Research Tool

A semi-structured interview guide served as the main research tool for gathering data and secondary data was also collected using academic literature, research studies, and other cybersecurity guidelines and frameworks. Open-ended questions about participant awareness of cybersecurity, experiences with digital dangers personally, and attitudes towards cybersecurity education were included in this guide to promote debate. Because of the semi-structured format's flexibility, we were able to delve deeper into subjects as they came up during conversations based on prompt replies by interviewees. Taken into consideration from the highly regarded book by Anderson and Whitman (2024), frequently used in academic settings offering a grounded framework for understanding cybersecurity concepts, best practices, and current threats; a few questions were considered as most important to ask students to check their cybersecurity awareness. The following crucial issues were the focus of the interviews:

- General awareness of cybersecurity vulnerabilities and risks: Students' comprehension of typical dangers such as ransomware, malware, phishing, and social engineering assaults.
- Awareness of cybersecurity best practices: Students should be able to identify phishing efforts, use multi-factor authentication, avoid dubious links, and manage secure passwords.
- Reporting of cybersecurity incidents: This section comprises the individual experiences of students' ability to report cybersecurity incidents, covering their reactions, the effects on their personal or academic lives, and any problems they faced in reporting or lessening the cybersecurity incidents.
- Perceptions of the university's cybersecurity education and support: Students' opinions regarding a handbook's suitability, the accessibility of resources for assistance, and their capacity to increase knowledge of cybersecurity issues.

### 3.6.3 Secondary Data

**Academic Literature and Research Studies:** According to Anderson and Whitman (2024), the rising frequency of cyberattacks has significant economic implications, especially for institutions that fail to implement adequate cybersecurity measures. Anderson and Whitman (2024) argue that despite the increasing number of cyberattacks, many students are not well-prepared to handle basic cyber threats like phishing and ransomware.

The EU's cybersecurity strategies emphasize the importance of awareness campaigns and training (ENISA 2022), particularly in higher education institutions. NIST (2021, 10-30) also highlights the

critical role that universities play in educating students about cybersecurity and suggests a comprehensive approach involving both theoretical and practical learning.

**Cybersecurity Guidelines and Frameworks:**

Existing guidelines, such as those from the National Cyber Security Centre (NCSC) or other cybersecurity best practice frameworks, were reviewed to understand standard recommendations for educational institutions on how to incorporate cybersecurity training into their curriculum. Guidelines on creating cybersecurity education programs for students, recommendations for creating awareness of common cyber threats like phishing, malware, and ransomware, and frameworks for improving overall security awareness in educational settings.

### 3.6.4 Getting the Interviews Started

A month was dedicated to conducting the focus group interviews. Every session was held in a calm, welcoming environment online to promote a candid conversation. Each session lasted between 30 to 40 minutes. A member of the research team steered the conversations during the interviews, making sure that each participant got a chance to express their opinions. The interview discussions were majorly prompt based; however, an interview guide was also used to steer the conversation to collect a productive set of data according to the research needs (see Appendix 1 for Interview Guide). To record notes and monitor group dynamics, which are critical for examining group interactions—after sharing research announcements with them and obtaining consent from participants, recordings were taken in online interviews to work on the data later.

### 3.6.5 Demographics of the interview participants

Participants included both bachelor's and master's students from various degree programs, ensuring a diverse range of perspectives on cybersecurity awareness. The focus group interviews for the thesis on enhancing cybersecurity awareness at Haaga Helia University of Applied Sciences included a diverse group of participants from various academic backgrounds. The participants included both bachelor's and master's students. The master's students were enrolled in programs such as Leading Business Transformation (LEBUM) and Business Technologies (BUTEM). Strategizing in Organizations (STROME), and Aviation & Tourism Business (ATBUM). The bachelor's students came from a range of programs, including Business Information Technology, International Business, Sustainable Aviation Business, and Digital Business Innovations etcetera. This mix of participants ensured a broad spectrum of perspectives and insights into cybersecurity awareness among students at different academic levels and fields of study.

## 3.7 Data Analysis

Thematic analysis, a popular technique for analysing qualitative data that focuses on finding and understanding patterns or themes within the data, was used to examine the information gathered from the focus group interviews (Braun & Clarke 2006, 77-101). There were multiple steps in the analysis:

### 3.7.1 Transcription

To guarantee accuracy in data representation, all interviews were verbatim transcribed after being recorded (with participants' consent).

### 3.7.2 Initial Coding

To create initial codes that captured key details about students' cybersecurity awareness, transcripts were reviewed one by one and analysed several times. The analysis combines insights from five interview datasets, each contributing to a comprehensive understanding of students' cybersecurity awareness, practices, and attitudes. Each interview transcript data was highlighted and quotes from interviewees were grouped separately with distinct colours. The use of a special software was considered unnecessary for analysing data as themes were identified from the amount of data to be analysed.

### 3.7.3 Themes

Thematic analysis, which includes finding patterns or themes within qualitative data, was used to examine the information gathered from focus group interviews (Braun & Clarke, 2006, 77-101). This approach made it possible to fully understand the demands, behaviours, and cybersecurity awareness of Haaga Helia pupils. Four broad themes that capture the main concerns expressed by participants were found once the data was coded:

a. Awareness and perception of barriers to cybersecurity
b. Real-life encounters with cyberthreats
c. Inconsistent and often weak security practices
d. Demand for clear and practical cybersecurity guidance

### 3.7.4 Results

**a) Awareness and Perception of Barriers to Cybersecurity**

**Summary**: The lack of cybersecurity awareness, particularly among non-IT students, was the most significant obstacle found in all the interviews. Participants reported having little understanding of the terms used in cybersecurity (such as ransomware, malware, and phishing) and their meanings.

While some students were ignorant of typical concerns, such as those connected to public Wi-Fi, many admitted that they hardly ever considered cybersecurity unless confronted with a direct threat.

**Key Findings:**

- Limited Understanding: Many students did not understand the specifics of cybersecurity, with terms like "ransomware" and "phishing" being unfamiliar.

Example: Focus Group 1 participant: *"I did not even know public Wi-Fi could be unsafe. I always just connect without thinking much about it."*

- Awareness of Targeted Threats: Despite low awareness, students recognized the education sector as a frequent target for cybercriminals, highlighting the need for better protection.

Example: Focus Group 3 participant: *"The education sector is a top target for cyber attackers."*

- Perceived Complexity: Cybersecurity was often seen as a subject too technical or specialized, making it less appealing to non-IT students.

Example: Focus Group 2 participant: *"I don't have any idea about cybersecurity."*

b) Real-Life Encounters with Cyber Threats

**Summary:** Despite gaps in awareness, almost all participants shared experiences with cyber threats, including phishing emails, malware, and scams. These encounters often led to heightened awareness and interest in cybersecurity, underscoring the importance of practical education. Incidents such as losing money to scams or dealing with ransomware in a professional setting revealed the tangible consequences of poor cybersecurity practices.

**Key Findings:**

- Personal Experiences with Attacks: Many students recounted experiences with phishing, scams, and even ransomware attacks, showing that awareness alone does not shield individuals from threats.

Example: Focus Group 5 participant: "I clicked on a link through a second-hand website and lost 200 euros in a scam."

- Prevalence of Cyber Incidents: The frequency of encounters with cyber threats was high, with many students experiencing phishing or scams directly affecting their personal or academic lives.

Example: Focus Group 1 participant: “Our healthcare IT company was hit with a ransomware attack that jeopardized patient data.”

- Trigger for Increased Awareness: Personal experiences often served as a wake-up call, motivating students to learn more about securing their digital presence.

Example: Focus Group 3 participant: “My LinkedIn account got hacked because I used the same password from Instagram.”

c) Inconsistent and Often Weak Security Practices

**Summary**: Inconsistent security practices were a common theme across all interviews. While some students adopted security measures like two-factor authentication (2FA), many others re-used passwords across multiple accounts or did not update passwords regularly. This inconsistency reveals a gap between students' theoretical knowledge of cybersecurity and their day-to-day security practices.

**Key Findings:**

- **Password Reuse and Weak Security Habits:** A considerable number of students admitted to reusing passwords or using weak password patterns for convenience, exposing themselves to higher risks.

Example: Focus Group 2 participant: *“I use the same password for almost everything, though I do have two-step verification.”*

- **Awareness of Best Practices vs. Implementation:** Some students were aware of the need to change their passwords and use more secure practices but found it difficult to implement them.

Example: Focus Group 4 participant: *“Honestly, I know I need to change my passwords, but I do not. It is just too hard to remember all of them.”*

- **Variability in Security Measures:** While some students employed strong security practices, others did not use simple measures like password updates or security warnings, leading to inconsistencies.

Example: Focus Group 1 participant: *“I use Google-suggested passwords that are difficult to guess, but I know I should be updating my passwords more often.”*

d) Demand for Clear and Practical Cybersecurity Guidance

**Summary:** The demand for a practical, student-friendly cybersecurity guide was a key subject. Students wanted straightforward, actionable information on how to protect themselves online. Suggestions for the handbook included making it visually engaging, interactive, and concise, with practical tips, examples, and quizzes. This was seen to bridge the gap between theoretical knowledge and practical application.

**Key Findings:**

- **Interest in Practical Resources:** All participants expressed interest in a handbook that would simplify cybersecurity concepts and offer actionable advice.

Example: Focus Group 3 participant: *"The handbook should include examples of fake links so students can understand what phishing looks like in practice."*

- **Visually Engaging and Interactive Content:** Participants emphasized the need for visually appealing content, such as images and diagrams, to make the information more digestible.

Example: Focus Group 2 participant: *"A handbook with examples of safe vs. unsafe links would be very useful."*

- **Topics for Handbook Inclusion:** There was consensus on the need for topics like phishing identification, password security, public Wi-Fi risks, and real-world examples of cyber threats.

Example: Focus Group 4 participant: *"Include examples of phishing email quotes showing what to avoid. It should start simple and build up."*

### 3.7.5 Examining Themes

After identification, the themes were examined and improved to make sure they correctly summarized the information and coordinated in the below table as per identified themes.

| Theme From Interviews | Description | Example Quotes |
|---|---|---|
| **Awareness and Perception Barriers** | Limited awareness among non-IT students; cybersecurity is often perceived as complex and specialized. | "I didn't know public Wi-Fi could be unsafe." (Focus Group 4)/ "I don't have any idea about cybersecurity." (Focus Group 1) |
| **Real-Life Encounters with Threats** | Participants met phishing, scams, and malware firsthand, highlighting a need for better prevention knowledge. | "I clicked on a link and lost 200 euros." (Focus Group 5) / "Our healthcare company faced ransomware affecting patient data." (Focus Group 2) |
| **Inconsistent Security Practices** | Password reuse and lack of security updates were common, with some students | "I don't change my passwords; it's too hard to remember all of them." (Focus Group 4) / "I just use the |

| | | |
|---|---|---|
| | ignoring recommended practices. | same password across platforms" (Focus Group 2) |
| **Demand for Practical Guidance** | Strong demand for a student-friendly cybersecurity handbook, with a focus on visual aids, practical examples, and interactive content to engage students. | "Include examples of fake links." (Focus Group 3) / "A short guide with visuals would make it easier to understand and apply cybersecurity principles." (Focus Group 2) |

### 3.8 Thesis Outcome

Gaining a better understanding of the cybersecurity awareness held by students was the main goal of the focus group interviews. Among the desired outcomes were:

- Pointing out certain areas where students believe their knowledge of cybersecurity dangers is lacking.
- Gaining knowledge of their experiences with cybersecurity events and how they handled them.
- Gaining knowledge on the best way to craft a cybersecurity awareness handbook to meet their needs.

The purpose of this qualitative investigation is to provide insights for the creation of instructional materials that improve students' cybersecurity practices and introduce them in the course curriculum of Haaga-Helia mandatorily so that students can be more self-aware about cyberthreats.

A thorough, student-focused short cybersecurity handbook that fills important knowledge, engagement, and practical application gaps in cybersecurity practices among Haaga-Helia students is the outcome of this thesis. This handbook covers basic cyber threats including ransomware, malware, and phishing and provides clear, simple, and visually appealing knowledge. It has educational videos, detailed instructions for creating secure passwords, and crucial advice on how to spot suspicious links and identify dangers on public Wi-Fi. To promote safer online practices among academics, this handbook is intended to be a useful educational resource that fits with students' requirements and preferences.

#### 3.8.1 Target Group of the Outcome

Students enrolled at Haaga Helia University of Applied Sciences are the handbook's main target audience. This covers students pursuing bachelor's and master's degrees in both technical and

non-technical fields. The handbook looks to improve students' personal and academic digital safety by addressing the cybersecurity issues pertinent to this diverse population and empowering them to make safer online decisions.

### 3.8.2 Problems and Needs Addressed by the Outcome

The following concerns are intended to be addressed by the cybersecurity awareness handbook created as part of this study:

- Low Cybersecurity Awareness: A lot of students are more susceptible to cyberattacks since they do not have a basic awareness of cybersecurity dangers including phishing, malware, and social engineering.
- Behavioural Risks: Students often engage in behaviours that put them and the school at risk, such as using the same passwords, connecting to unprotected public Wi-Fi networks, and not seeing phishing efforts.
- Practical Education Gap: If cybersecurity training programs exist, they are often viewed as being overly technical or unrelated to students' daily interactions as per data collected in the focus group interviews. This emphasises the necessity of a useful, relatable, and student-centred resource.

The handbook provides clear, practical, and aesthetically pleasing information on important cybersecurity practices to close these gaps.

### 3.8.3 Expectations and Evaluation of the Outcome

The study was intended to yield a useful result that would be pertinent and helpful to Haaga Helia's student body, even if the organisation did not formally commission it. When creating and assessing the handbook, the following standards were considered:

- **Relevance and Applicability:** The guidebook addresses basic cybersecurity concerns that students meet daily, such as phishing awareness, secure password habits, and safe public Wi-Fi usage.
- **Usability and Accessibility:** The handbook is made to be brief, visually appealing, and easy to use so that a variety of students can find it appealing.
- **Practicality:** To aid students in successfully implementing best practices, the content contains examples, real-world examples, and practical advice.
- **Development Process:** The material was shaped in large part by the insights gained from student focus groups, which helped to ensure that it reflected their unique requirements and preferences.

- **Evaluation Criteria:** The effectiveness of the handbook will be assessed according to its usability, content clarity, and ability to increase student awareness. Feedback from a pilot group of instructors and students may be included in this assessment in the future.

The goal of the project is to provide a resource that encourages a safer and better-informed digital culture by customising the handbook to the cybersecurity requirements of Haaga Helia's student body.

### 3.9 Data Management Plan

A research announcement was made, and informed consent was obtained from all participants, guaranteeing confidentiality and anonymity. Audio recordings of the interviews were securely stored and accessible only to the research team. Data was anonymized to protect participants' identities, and all personal identifiers were removed before analysis. The recorded data will be disposed of within 2 months of thesis submission.

# 4 Development Task

The development task's goal was to close the knowledge gap found during the research phase by producing an approachable, useful, and short cybersecurity handbook for Haaga Helia students (see Appendix 2 for the handbook). The handbook's goals are to raise students' knowledge of online dangers, develop their cybersecurity abilities, and encourage safe online conduct. This resource looks to demystify cybersecurity and give students the tools they need to defend themselves in increasingly complicated digital environments by providing straightforward, practical advice.

## 4.1 Needs Assessment & Research Basis

To inform the content and format of the handbook, a thorough needs assessment was conducted through secondary data by literature review and qualitative data collection including focus group interviews. Four key themes appeared: limited cybersecurity awareness, inconsistent security practices, real-life experiences with cyber threats, and a strong demand for clear, practical guidance. Each theme provided insight into the specific challenges students face and informed the handbook’s structure. For instance, participants’ requests for straightforward explanations and practical examples led to a decision to include scenarios that mimic real-life encounters with phishing frauds, insecure Wi-Fi networks, and password management challenges.

## 4.2 Design and Content Development Process

Using a user-centred design methodology, the handbook's creation prioritized readability, accessibility, and engagement. Simple language, relatable examples, and modular parts that students may read on their own according to their requirements were given priority in the first content versions. Additionally, the design considered suggestions made by interviewees, who emphasized the importance of concise instructions for comprehension. To promote active learning and reinforce important concepts, interactive features like QR codes that link to online videos were also incorporated. Moreover, the information and suggestions offered were chosen by the application of development methods, as described in research by Vance et al. (2012). The key steps in Handbook development include:

### 4.2.1 Planning and Initial Drafts

- The needs assessment's conclusions served as the foundation for the first content outlines.
- Common cyber threats, workable remedies, and real-world applications were among the main areas of focus.

- The content was written with readability in mind, utilising relatable examples and simple language.

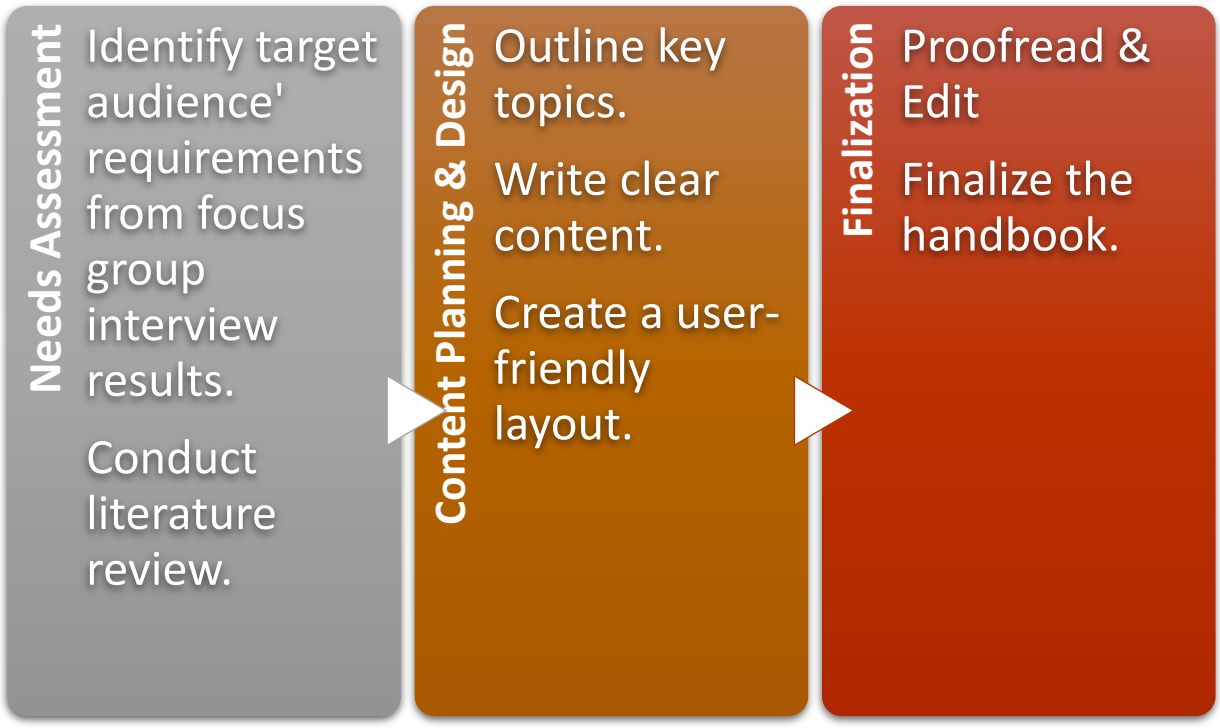
### 4.2.2 Visual and Interactive Design

- The design used visual aids like infographics to simplify complicated concepts, drawing inspiration from Vance et al. (2012).
- To encourage active learning, interactive features were included, such as QR codes that led to video courses.

### 4.2.3 Finalization of Handbook Content

- Proofreading and Editing: Ensuring the accuracy and consistency of the content.
- Future Steps: Taking opinions from industry experts on the handbook and distributing the handbook to students through various channels, such as the university website, email, and physical copies for comments on possible future versions.

**Development Task Flowchart:**




The cybersecurity handbook's goal is to equip Haaga Helia pupils with the information and abilities needed to safely and responsibly traverse the digital world by adhering to this exacting development procedure.

### 4.3 Handbook Structure and Content

As per Vance et al. (2012), a handbook places significant emphasis on workable measures that students can implement to enhance their cybersecurity practices. Adding visual aids, useful advice, and real-world examples improves comprehension and engagement while simplifying difficult ideas. Cybersecurity handbooks (ClearTwo 2024) were taken as role models in designing the topics and overall layout of the handbook. After the data analysis stage, famous books like the one by Anderson & Whitman 2024, were used as references to craft a content and concise handbook accordingly. The handbook covers essential cybersecurity topics, including:

- Common Cyber threats and vulnerabilities
- Best practices for online safety
- Password management
- Social engineering tactics
- Phishing scams
- Malware prevention
- Protecting digital assets
- Resources & Tools

# 5 Discussion

## 5.1 Overview

In this chapter, the study findings are discussed in relation to the thesis objectives, their consequences are interpreted, and the evolution of the cybersecurity handbook is reflected. It discusses the discovery's wider importance and suggests ideas for additional investigation. This chapter presents a summary of results considering the results in relation to the theoretical framework and then evaluates the outcome as conclusions in terms of timeliness, necessity, and usability.

## 5.2 Summary of Key Findings

The main conclusions about students' awareness and usage of cybersecurity are examined in this section. Important topics to talk about include:

- Awareness of Cybersecurity in General: The study found that although most students recognise the value of cybersecurity, their knowledge is frequently restricted to fundamental ideas like data privacy and password management. This identifies a knowledge gap in cybersecurity, which the handbook attempts to fill by offering advanced advice for a range of skill levels along with core principles.
- Diversities in Cybersecurity Procedures: The results showed that students' approaches to cybersecurity varied widely, with those who are less tech-savvy displaying erratic behaviours and low self-confidence in their abilities to manage online threats. The concise design of the handbook, which prioritises clarity and useful advice for typical situations students see on a regular basis, was influenced by this discrepancy.

## 5.3 Institutional Impact

By providing clear, useful advice for all students, regardless of background, the handbook closes a gap. It uses relatable language and real-world examples to help all students especially non-IT students form safe internet habits. Because of this interdisciplinary approach, everyone on campus can benefit from knowing about cybersecurity.

## 5.4 Limitations and Challenges

A small sample size and the difficulty of striking a balance between accessibility and technical accuracy are among the limitations. Although the results influenced the handbook's creation, more testing with a bigger sample size could improve it even more in the future.

## 5.5 Recommendations for Future Research

Future studies should examine how well the handbook works in various media, like interactive or digital editions. Further research might examine the potential benefits of gamified courses and other customised content for increasing student engagement and knowledge retention.

# 6 Conclusion

## 6.1 Summary

The goal of this thesis was to address the urgent demand for hands-on cybersecurity education by developing an approachable cybersecurity handbook for a wide range of students. A resource created to accommodate multiple knowledge levels while maintaining universal applicability was informed by qualitative research, which revealed insights into students' diverse cybersecurity practices and understanding.

## 6.2 Contributions to Cybersecurity Education

The handbook bridges a resource gap and promotes safe digital practices by making cybersecurity education accessible to students across all subject areas. It is a useful tool that may be included in school campaigns, student forums, and various curriculum courses to raise awareness of cybersecurity.

## 6.3 Broader Implications

The handbook could be a useful resource for academic institutions, helping to create a campus culture that is safer and more responsible with technology. Encouraging safer digital activities across the campus, helps institutions cultivate a culture of cybersecurity awareness and gives students the power to make educated decisions online.

## 6.4 Future Improvements

Specialized information for various student groups and interactive forms for increased interaction could be included in future editions.

## 6.5 Final Reflection

This thesis emphasizes how crucial it is to give all students a baseline understanding of cybersecurity, regardless of their field of study. The handbook helps students become more proactive in safeguarding themselves in an increasingly complex digital world, which is an important step in fostering digital safety and accountability. The handbook is an essential tool in the larger framework of cybersecurity education and awareness since it gives students the confidence they need to manage cyberspace.

## References


1. Aalto University. 2018. *Challenges in Implementing Cybersecurity Education in Academic Institutions*. Available at: https://research.aalto.fi/en/publications/challenges-in-cybersecurity.
2. Ajzen, I. 1991. The theory of planned behaviour. Organizational Behaviour and Human Decision Processes, 50(2), 179–211. DOI: https://doi.org/10.1016/0749-5978(91)90020-T
3. Anderson, J.A. and Whitman, M.E. 2024. *Cybersecurity: A Comprehensive Guide*. Hoboken, NJ: Wiley.
4. Bandura, A. 1989. Human agency in social cognitive theory. Available at: https://psycnet.apa.org/record/1990-01275-001.
5. Bandura, A. 2001. Social Cognitive Theory: An Agentic Perspective. *Annual Review of Psychology*, 52, pp.1–26. URL: https://www.annualreviews.org/content/journals/10.1146/annurev.psych.52.1.1.
6. Bhattacherjee, A. (2016). Cybersecurity in higher education: A comprehensive review. Computers & Security, 58, 1-16.
7. Blakley, B., Frincke, D. and Smith, R. 2001. Security Education: The Key to Reducing Risks. *Computer Security Journal*, 17(2), pp.31–41.
8. Bottyan, L. 2023. Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences*, 13, pp.1–11. DOI: https://doi.org/10.24368/jates363.
9. Braun, V. and Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), pp.77–101.
10. Braun, V. and Clarke, V. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3(2), pp.77–101.
11. Chabrow, E. 2014. 5 Things You Should Know About Cybersecurity Awareness Training. *InformationWeek*. Available at: www.informationweek.com.
12. Chaudhary, S., Gkioulos, V. and Katsikas, S. 2022. Developing Metrics to Assess the Effectiveness of Cybersecurity Awareness Program. *Journal of Cybersecurity*, 8(1). DOI: https://doi.org/10.1093/cybsec/tyac006.
13. Cherry, K. 2023. What is reciprocal determinism? *Verywell Mind*. Available at: https://www.verywellmind.com/what-is-reciprocal-determinism-2795907.
14. Cleartwo. 2023. *Cybersecurity: A Guide for Businesses*. Available at: https://cleartwo.co.uk/cybersecurity-a-guide-for-businesses/.
15. Coghlan, D. and Brannick, T. 2014. *Doing Action Research in Your Own Organization*. 4th ed. London: Sage.

16. Council of Europe (2020). Recommendations for Cyber Security Awareness Raising in Higher Education Institutions. URL: *https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states*
17. Creswell, J.W. and Creswell, J.D. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. Thousand Oaks, CA: Sage.
18. Creswell, J.W. and Poth, C.H. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. Thousand Oaks, CA: Sage. Available at: https://edge.sagepub.com/creswellrd6e
19. Davis, F. D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008
20. Deci, E. L. & Ryan, R. M. 2000. The "what" and "why" of goal pursuits: Human needs and the self-determination of behaviour. Psychological Inquiry, 11(4), 227–268. https://doi.org/10.1207/S15327965PLI1104_01
21. European Union Agency for Cybersecurity (ENISA). (2022). *Cybersecurity education and awareness in Europe: Trends and challenges*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-education
22. European Union Agency for Cybersecurity. (2022). EU Cybersecurity Strategy.
23. Firmansyah, D. and Saepuloh, D. 2002. *Social Learning Theory: Cognitive and Behavioural Approaches*. Available at: https://www.researchgate.net/publication/367220348_Social_Learning_Theory_Cognitive_and_Behavioural_Approaches.
24. General Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
25. Haaga Helia University of Applied Sciences (2023). *About Haaga Helia.* URL: https://www.haaga-helia.fi
26. Hadnagy, C. 2018. Social Engineering: The Science of Human Hacking. Hoboken, NJ: Wiley.
27. Herr, K., and Anderson, G.L. 2015. The Action Research Dissertation: A Guide for Students and Faculty. 2nd ed. London: Sage.
28. Kemmis, S. and McTaggart, R. 2018. *The Action-Research Planner: A Guide to Improving Practice*. 4th ed. London: Routledge. Available at: https://www.routledge.com/The-Action-Research-Planner/Kemmis-McTaggart/p/book/9781138536355
29. Kemmis, S., McTaggart, R. and Nixon, R. 2014. *The Action Research Planner: Doing Critical Participatory Action Research*. Singapore: Springer. Available at: https://www.springer.com/gp/book/9789814560672

30. Lee, H.-S., Flores, L.Y., Navarro, R.L. and Kanagui-Muñoz, M. 2015. A longitudinal test of social cognitive career theory's academic persistence model among Latino/a and White men and women engineering students. *Journal of Vocational Behaviour*, 88, pp.95–103. DOI: https://doi.org/10.1016/j.jvb.2015.02.003.
31. Lewin, K. 1946. Action Research and Minority Problems. *Journal of Social Issues*, 2(4), pp.34–46.
32. Li, Q., Wang, H., & Zhang, Y. (2019). Cybersecurity awareness among college students: A systematic review. Computers & Security, 82, 101431.
33. Li, X., Zhu, Y., & Chen, J. (2019). *Cybersecurity awareness among university students: Current state and gaps.* Computers in Education, 27(4), 234–250.
34. Miller, S.A., Overstreet, L. and Lang, D. 2022. Social Learning Theory: Observational Learning. *iastate.pressbooks.pub*. Available at: https://iastate.pressbooks.pub/individual-familydevelopment/chapter/social-learning-theory-observational-learning/.
35. Moallem, A. 2019. Cyber Security Awareness Among College Students. In: T. Z. Ahram & D. Nicholson, eds. *Advances in Human Factors in Cybersecurity*. Cham: Springer International Publishing, pp.79–87. DOI: https://doi.org/10.1007/978-3-319-94782-2_8.
36. Moodle (2023). *Security and Privacy Policies.* URL:https://moodle.org/security
37. National Cyber Security Centre (NCSC). (2020). *Cybersecurity training and education: A framework for universities*. National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/university-cybersecurity-guide
38. National Cyber Security Centre (NCSC-FI). 2023. *The Finnish Threat Landscape Report*. Available at: https://www.kyberturvallisuuskeskus.fi/en/our-services.
39. National Institute of Standards and Technology (NIST). (2021). *National cybersecurity awareness month: Promoting cybersecurity education in academia*. NIST. https://www.nist.gov/cybersecurity-awareness
40. National Institute of Standards and Technology. (2021). Cybersecurity Framework.
41. Nickerson, C. 2024. Albert Bandura's Social Cognitive Theory. *Simply Psychology*. Available at: https://www.simplypsychology.org/social-cognitive-theory.html.
42. OECD. (2018). Artificial intelligence in education: A review of the state of the art. OECD
43. Pajares, F. 2002. *Overview of Social Cognitive Theory and of Self-Efficacy*. Available at: https://people.wku.edu/richard.miller/banduratheory.pdf.
44. Reason, P. and Bradbury, H. 2008. The SAGE Handbook of Action Research: Participative Inquiry and Practice. 2nd ed. London: Sage.
45. Rogers, R. W. 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. New York: Guilford Press.

46. Sagor, R. 2011. The Action Research Handbook: A Four-Stage Process for Educators and School Teams. 2nd ed. London: Sage.
47. Scheponik, T., Sherman, A.T., DeLatte, D., Phatak, D., Oliva, L., Thompson, J., and Herman, G.L. 2016. How students reason about Cybersecurity concepts. *IEEE Frontiers in Education Conference (FIE)*. DOI: https://doi.org/10.1109/FIE.2016.7757363.
48. Schunk, D.H. 2012. *Learning Theories: An Educational Perspective*. 6th ed. Boston: Pearson. Available at: https://www.researchgate.net/profile/Ana-Maria-Ciobotaru/post/Good-Books-on-Teaching-Methods/attachment/59d61dce79197b807797a03c/AS%3A273549456019456%401442230680395/download/%5BDale_H._Schunk%5D_Learning_Theories_An_Educational..pdf.
49. Schunk, D.H. and Pajares, F. 2010. Self-efficacy beliefs in academic settings. *International Encyclopedia of Education*. Available at: https://www.sciencedirect.com/science/article/abs/pii/B9780080448947006205.
50. Six, H. 2024. *Cyber Awareness: The Psychology of Behaviour Change*. Hut Six. Available at: https://www.hutsix.io/cyber-awareness-the-psychology-of-behaviour-change-part-1.
51. SoSafe. 2023. *Benefits of Behavioural Science in Cyber Security Training*. Available at: https://sosafe-awareness.com/blog/the-top-5-benefits-of-applying-behavioural-science-to-cyber-security-awareness-training/.
52. Stone, S. 2017. Observational learning. In: *Encyclopædia Britannica*. Available at: https://www.britannica.com/science/observational-learning.
53. Stringer, E.T. 2023. *Action Research: A Practical Guide*. 5th ed. London: Sage.
54. Sweeney, L. (2018). Students' cybersecurity behaviours: A review of the literature. Computers & Education, 125, 130-141.
55. Tamrin, S.I., Norman, A.A. and Hamid, S. 2021. Intention to share: The relationship between cybersecurity behaviour and sharing specific content on Facebook. *Information Research*. Available at: https://informationr.net/ir/26-1/paper894.html.
56. TSC. 2023. *The Bandura Effect: How to Harness this Powerful Behaviour Model in Your Training*. Available at: https://thesecuritycompany.com/the-insider/the-bandura-effect-how-to-harness-this-powerful-behaviour-model-in-your-training/.
57. University of Helsinki. 2024. *National Cybersecurity Education and Training Initiatives*. Available at: https://studies.helsinki.fi/courses/course-implementation/otm-92500492-f6c6-4dba-8313-768993a0ede9.
58. University of Jyväskylä. 2016. Cyber Security Education and Research in Finland's Universities and Universities of Applied Sciences. *International Journal of Cyber Warfare and Terrorism*. Available at: https://www.researchgate.net/publication/303092874. DOI: 10.4018/IJCWT.2016040102.

59. Vance, A., Siponen, M. and Pahnila, S. 2012. Feasibility of Information Security Awareness Training: An Empirical Study. *Information & Computer Security*, 20(4), pp.307–321.
60. William, J. 2022. Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability*, 3(1), pp.47–67. DOI: https://doi.org/10.52889/ijses.v3i1.13.
61. Yin, R.K. 2025. *Case Study Research: Design and Methods*. 7th ed. Thousand Oaks, CA: Sage.
62. Zimmerman, B.J. 2000. Attaining Self-Regulation: A Social Cognitive Perspective. In: M. Boekaerts, P.R. Pintrich, & M. Zeidner, eds. *Handbook of Self-Regulation*. San Diego: Academic Press, pp. 13–39. DOI: 10.1016/B978-012109890-2/50031-7.

# Appendices

### Appendix 1. Interview Guide:

The interview guide used for the focus groups with Haaga-Helia University students to gauge their understanding of cybersecurity is included in this appendix. The purpose of the guide was to gather productive information from students regarding their knowledge of cybersecurity risks, best practices, and individual encounters with cyberthreats.

The interviewer's opening statement:
The thesis topic is introduced. The interviewee's anonymity is explained. Do you have any queries before we begin? Accepting the possibility of recording the interview.

**Interview Questions:**

Can you introduce yourself briefly to the group and share your current level of knowledge on cybersecurity?

How do you usually respond to shady/suspicious email messages or links? Are you able to identify if it is shady?

Can you distinguish between phishing, malware, and ransomware?

Are you taught about cybersecurity in your current course or job? How do you think it could be improved?

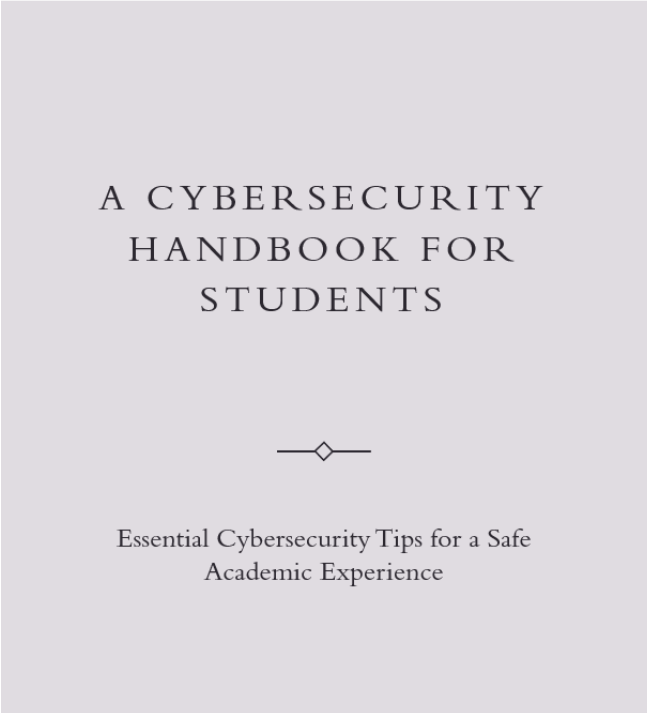
What do you think is the best approach? Using the same password for multiple accounts or different passwords for each?

What was your response when you encountered a cybersecurity incident?

How important do you think cybersecurity education is for students and why?

What should a cybersecurity handbook include? How long should it be?

**Appendix 2. Glimpses of the outcome of the thesis- Cybersecurity Handbook for Students (PDF)**




Haaga-Helia

## Table of Contents

## *Preface:* News on a Recent Cybersecurity Attack on Students' Data!

An attempt had been made recently to hack into Haaga-Helia's mainly student accounts, which had caused the accounts to be locked. The lock was on for a certain period of time and the accounts could not be used at that time. (Source: https://www.haaga-helia.fi/en/current/news/targeted-attack-against-user-identification-updated-276)


*Source:* https://www.haaga-helia.fi/en/current/news/targeted-attack-against-user-identification-updated-276

## *Getting to know Cybersecurity Basics*

### *What is Cybersecurity?*

- Defeding data, networks, and systems against online threats.

### *Why does it matter?*

- Common cyberthreats such as phishing, malware, and account hacking can jeopardise your academic work, funds, and privacy as well.


***Phishing:*** A practice of sending fake emails or texts that appear to be from reliable sources to obtain your personal information or login credentials.

***Example:*** "Your Outlook account is blocked by Haaga-Helia. Click ***here*** to unblock your email."

***Spear Phishing:*** A more targeted phishing by someone known to the target where the attacker tailor messages specifically to an individual.

***Example:*** Hello John Doe. Please change your password of your outlook account by clicking ***here***.

Scan or open the below Youtube Video link to know more about common types of phishing attacks: https://youtu.be/rb26NK0jtHM?si=_KD16Ye-x7GLhmYC

## *Viruses*

They often spread through shared files, network drives, or email attachments, interfering with class work and erasing data.

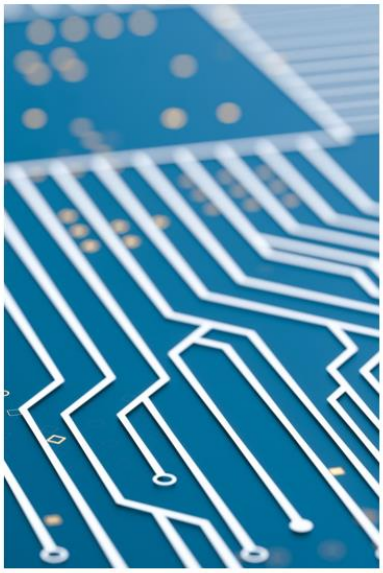
***Example:*** Assume that a teacher sends a digital file to you, such as a practice test or another student share files with you over email. If you downloads a file that has a virus attached to it without realization, the virus may infect your device and subsequently other devices on the same network or shared storage.

*Scan the link or open the below Youtube Video link to know more about common types of Malware attacks: https://www.youtube.com/watch?v=n8mbzU0X2nQ*

## *Worms*

These are standalone self-replicating softwares that can spread across networks, causing a system overload.

***Example***: Think of a computer virus that attacks PCs in a communal lab or library. The worm could spread among the lab's network-connected gadgets if one student unintentionally introduces it by downloading an infected file or connecting in an infected USB drive. Students working on assignments or lab research may be impacted by device shutdowns, sluggish reaction times, and possible data loss.



## *Trojans- Malware disguised as a legitimate software*

Trojan horses pose as trustworthy programs and once installed, provide hackers access to networks without authorization. This can result in the theft of private data, such as student information or academic records.

***For instance, fraudulent academic software Trojan:*** A student may download a "free" version of academic software (such Microsoft Office or SPSS) or what looks to be a genuine study app or online textbook. On the other hand, if it's a trojan, it might give an attacker backdoor access. After gaining access to the student's files, the attacker might be able to steal login information for university accounts or keep an eye on device activity.

Ransomware attacks often begin with a phishing email, tricking a faculty member into clicking a malicious link or downloading an infected attachment. Once inside, the ransomware spreads, locking down access to student records, research data, and online coursework. This can disrupt classes, delay exams, and threaten research, especially in grant-funded projects.

In June 2020, University of California, San Francisco (UCSF) was targeted in a ransomware attack that encrypted a portion of its academic data. UCSF was forced to pay over $1.1 million in ransom to regain access to its encrypted data, as it was critical for some of their medical research. (Source: https://www.bbc.com/news/technology-53214783)

This attack shows the potentially high stakes for universities and the significant financial and operational impacts ransomware can have in an academic environment.

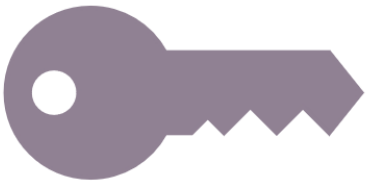
## *Social Engineering*

***Pretexting***: Tricking someone by faking a scenario to reveal confidential information. (E.g.: pretending to be IT support asking for login credentials.)

***Baiting***: Luring someone to leak information by offering something in return. (E.g.: Fake rewards or promise of free downloads)


## *Strong Passwords*

- Make use of lengthy passwords with a minimum of 12 characters that combine capital and lowercase letters, digits, and special characters.
- Refrain from using information that is readily guessed, such as names or birthdays.
- Password Manager: To prevent recycling complicated passwords across accounts, use a reputed password manager.



## *Multi-Factor Authentication (MFA)*

- Boost security by using MFA, which requires 2 different kinds of identification: your password plus a second factor, such as a code sent to your phone.
- Typical techniques include using biometric information (fingerprint, facial recognition), an authentication app (like Microsoft Authenticator), or an SMS with a code.
- To prevent unwanted access, enable 2FA for all significant accounts, including social media, banking, and email.

## *Beware of Public Wi-Fi*

- Steer clear of using unprotected public Wi-Fi networks (such as those found in coffee shops and airports) to access private information like bank accounts or personal information.
- When connecting to public Wi-Fi, use a virtual private network, or VPN, to encrypt your data and shield it from possible prying eyes.
- Turn off file sharing on open networks to shield your device from unwanted access.

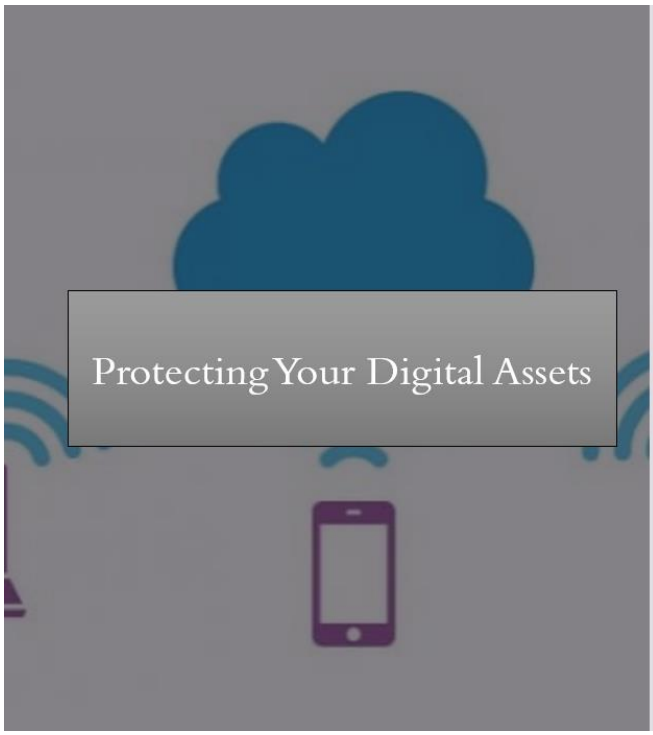
## *Regular Software Updates*

Update your devices and software to ensure you have the most recent security patches, which will shield you from known vulnerabilities.

Whenever possible, configure/set your devices to update automatically.

## Avoid Phishing Scams

- Watch out for dubious emails, attachments, or links from senders you don't recognize.
- Before downloading any files or clicking on any links, especially if they appear too good to be true or demand immediate action, make sure the source is reliable.
- Keep an eye out for phishing warning indicators, such as misspelt URLs, weird requests, or suspicious sender addresses.
- Hover over links before clicking.
- Be cautious of someone wanting you to do something urgently.




- Update system and apps frequently.
- Use biometrics, passwords, or PINs to secure devices.
- Store backup data in safe places.
- Don't share too much private information on social media.
- Make use of account privacy settings.
- Only connect with people you might know on school social media apps.
- Regularly back up your important files to an external hard drive or cloud storage.
- In case of a ransomware attack or data loss, you can recover your files from backup without paying a ransom.

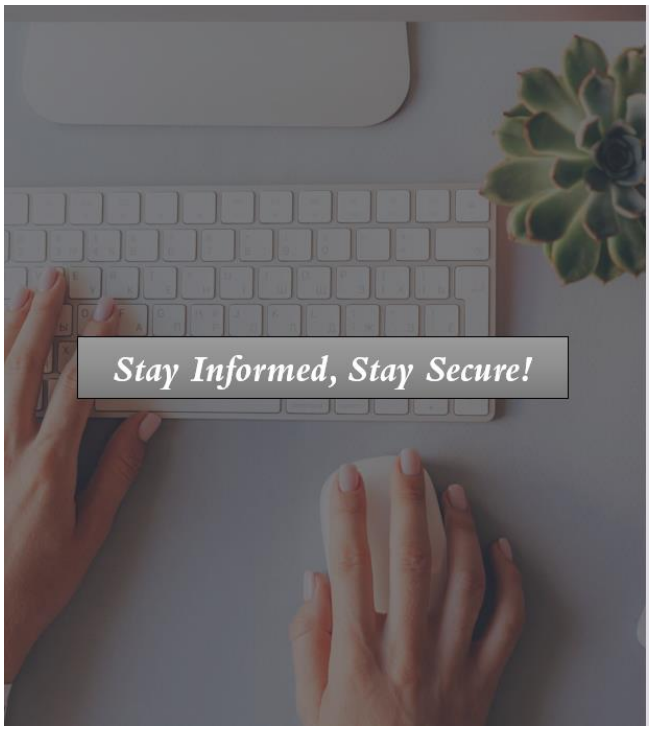
## *What to Do If You're Compromised*

| | |
|---|---|
| Suspect Phishing? | • Report it to Haaga-Helia IT staff and don't reply. |
| Account Hacked | • Enable MFA and change the password. |
| Infected Device | • Disconnect the infected device and do an antivirus scan. |

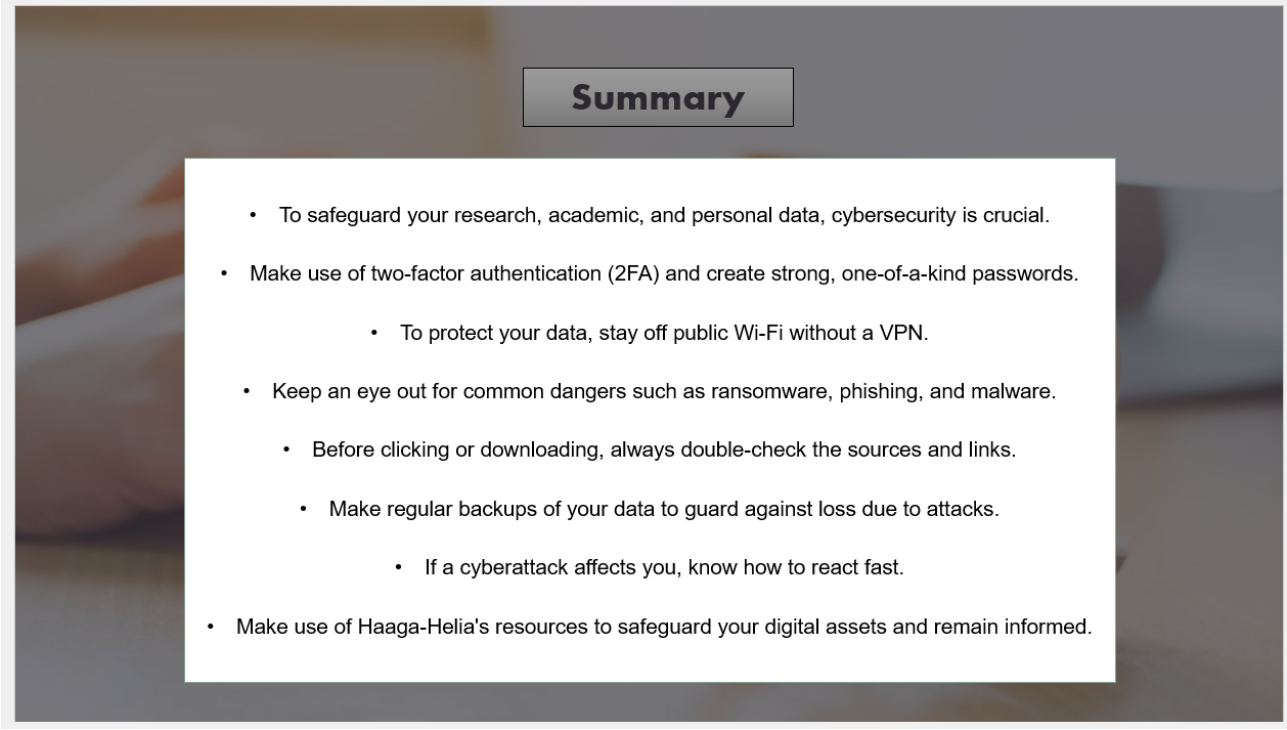

## Resources & Tools for Haaga-Helia Students

| | | | |
|---|---|---|---|
| By Email: helpdesk@haaga-helia.fi | By Phone: +358 – 080097750 | Pasila Campus: Room 5018 (Mon–Fri 12–12:45 pm) | The Hague Campus: Room A334 (Mon–Fri 9 am–3 pm) |

| | | |
|---|---|---|
| Malmi Campus: Room 404 (Mon–Fri at 12–1 pm) | Porvoo Campus: Info desk (Mon–Fri 9 am–3 pm), Room 1402 (Mon–Fri 12:15–13:00) | ***Check the strength of your passwords:*** https://www.haaga-helia.fi/en/study/student-user-ids-and-passwords |




- **Remain Alert:** Cyberthreats are ever-changing. It's critical to remain mindful of the dangers and take preventative action to safeguard your academic and personal data.
- **Your Online Persona Is Important:** Cybercriminals are interested in your intellectual property, research, academic records, and personal information. It is your duty to keep them safe.
- **Keep Your Defences Up:** Verify before clicking, downloading, or sharing critical information, and exercise caution while interacting with digital content, including emails, websites, and applications.
- Read this HBR article to know why cybersecurity is not only an IT department's issue to solve, but an enterprise-wide issue to address: https://hbr.org/2016/10/good-cybersecurity-doesnt-try-to-prevent-every-attack


Summary
• To safeguard your research, academic, and personal data, cybersecurity is crucial.
• Make use of two-factor authentication (2FA) and create strong, one-of-a-kind passwords.
• To protect your data, stay off public Wi-Fi without a VPN.
• Keep an eye out for common dangers such as ransomware, phishing, and malware.
• Before clicking or downloading, always double-check the sources and links.
• Make regular backups of your data to guard against loss due to attacks.
• If a cyberattack affects you, know how to react fast.
• Make use of Haaga-Helia's resources to safeguard your digital assets and remain informed.