TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Institute of Software Sciences
E-Governance Technologies and Services

Anastasiia Shapran 163037IVGM

EMPOWERING HIGH SCHOOL STUDENTS IN CYBERSECURITY: A MULTI-DIMENSIONAL APPROACH (THE CASE OF ONE ESTONIAN SCHOOL)

Master's Thesis

Supervisor: Olaf Manuel Maennel
PhD

Co-supervisor: Oleg Shvaikovsky
MSc, MBA

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Tarkvarateaduse Instituut
E-riigi tehnoloogiad ja teenused

Anastasiia Shapran 163037IVGM

GÜMNAASIUMIÕPILASTE KÜBERTURVALISUSE ALASTE TEADMISTE ARENDAMINE: MULTIDIMENSIONAALNE LÄHENEMINE (JUHTUMISUURING ÜHE EESTI KOOLI NÄITEL)

Magistritöö

Juhendaja: Olaf Manuel Maennel
PhD

Kaasjuhendaja: Oleg Shvaikovsky
MSc, MBA

Tallinn 2025

Author's Declaration of Originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Anastasiia Shapran

12.05.2025

Acknowledgements

The author of this thesis expresses sincere gratitude to the supervisor, Professor Olaf Manuel Maennel, and the co-supervisor, Oleg Shvaikovsky, MSc, MBA, for their respectful attitude, confidence-building, and continuous support throughout the writing of this thesis.

Special thanks are also extended to the Program Director of "E-Governance Technologies and Services", Professor Ingrid Pappel, and Tallinn University of Technology for providing a high level of instruction and a modern, forward-looking academic environment. Also, special thanks to Sille Arikas, MSc, whose passion for cybersecurity served as an inspiration to explore the field in depth. The way she taught cybersecurity courses at TalTech, including Foundations of Cyber Security, Cyber Security Management, and the Special Course in Cyber Security II, was both thoughtful and effective. Her practical homework assignments and the engaging study visits offered great insights into the industry. This experience significantly impacted the author's academic direction and future career plans.

The author also wishes to thank all the experts, the administration of Püha Johannese Kool, and the school teachers who generously contributed to this study despite their busy professional schedules. Their time, openness, and willingness to share experiences added meaningful perspectives to the research and enriched its authenticity.

Ultimately, the author deeply thanks her family for their patience, understanding, and emotional support during the most challenging phases of this academic journey.

Abstract

This Master's thesis examines the current status and possibilities of cyber security education in upper secondary schools (gymnasiums) on the example of one Estonian private school. The study looks at the problem through a multidimensional approach and considers cultural, technical, pedagogical, ethical and social-engineering aspects. The empirical part includes interviews with experts, a phishing simulation among IT and non-IT direction 12th graders and a classroom observation of IT direction 12th graders. The study conducted in the spring of 2025 reveals significant differences in cybersecurity awareness between student groups, highlights the impact of specific cybersecurity courses and the need for systemic and interdisciplinary integration of cybersecurity topics and digital competencies into general education.

In addition to exploring student knowledge and behaviour, the thesis examines barriers teachers face, ethical issues in teaching cybersecurity, and the importance of programming as a supporting skill. Experts' opinions describe the current situation on the labour market in cybersecurity and recommendations to the school community and students. In the final part, the research questions are answered and recommendations for policymakers, schools, and students are made, emphasising the role of a multidimensional approach, public-private partnerships, and hands-on learning methods. The research concludes that empowering students in cybersecurity requires not only technical training but also consideration of ethical principles and cultural awareness in a digital context. With the introduction of AI in education at the state level in Estonia, more effort should be made to develop critical thinking from school.

This thesis is written in English and is 81 pages long, including 5 chapters, 7 figures and 2 tables.

Keywords: High school students, Digital competence, Phishing simulation, K-12 education, ICT curriculum, Cyber hygiene, Estonia.

Annotatsioon

Gümnaasiumiõpilaste Küberturvalisuse Alaste Teadmiste Arendamine: Multidimensionaalne Lähenemine (Juhtumisuuring Ühe Eesti Kooli Näitel)

Käesolevas magistritöös uuritakse küberturvalisuse õpetamise hetkeseisu ja arendusvõimalusi gümnaasiumiastmes ühe Eesti erakooli näitel. Uurimistöös rakendatakse mitmemõõtmelist lähenemisviisi, võttes arvesse kultuurilisi, tehnilisi, pedagoogilisi, eetilisi ja sotsiaaltehnilisi aspekte. Empiiriline osa hõlmab ekspertintervjuusid, andmepüügi simulatsiooni IT- ja mitte-IT-suunaga 12. klassi õpilaste seas ning IT-suunaga klasside vaatlusi. 2025. aasta kevadel läbi viidud uuring toob esile märkimisväärseid erinevusi õpilasrühmade küberturvalisuse teadlikkuses, rõhutab spetsialiseeritud küberturvalisuse kursuste mõju ning osutab vajadusele küberturvalisuse teemade ja digipädevuste süsteemseks ja interdistsiplinaarseks lõimimiseks üldharidusse.

Lisaks õpilaste teadmiste ja käitumise analüüsile käsitletakse töös ka õpetajate ees seisvaid takistusi, eetilisi küsimusi küberturvalisuse õpetamisel ning programmeerimisoskuse rolli toetava pädevusena. Ekspertide hinnangud kirjeldavad valdkonna olukorda tööturul ning sisaldavad soovitusi koolikogukonnale ja õpilastele. Lõpuosas vastatakse uurimisküsimustele ning esitatakse soovitused hariduspoliitika kujundajatele, koolidele ja õppijatele, rõhutades mitmemõõtmelise lähenemisviisi, avaliku ja erasektori partnerluse ning praktiliste õpimeetodite olulisust. Uuringu tulemused näitavad, et õpilaste võimestamine küberturvalisuse vallas eeldab lisaks tehnilistele oskustele ka eetiliste põhimõtete ja kultuuriteadlikkuse arvestamist digitaalses kontekstis. Seoses tehisintellekti kasutuselevõtuga hariduses riiklikul tasandil Eestis tuleks kriitilise mõtlemise arendamisele pöörata rohkem tähelepanu juba kooliastmes.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 81 leheküljel, sealhulgas 5 peatükki, 7 joonist, 2 tabelit

Märksõnad: Gümnaasiumiõpilased, Digipädevus, Andmepüügisimulatsioon, Üldharidus, IKT õppekava, Küberhügieen, Eesti.

List of Abbreviations and Terms

AI	Artificial Intelligence
AI Leap 2025	National AI Education Programme in Estonia (*TI-Hüpe 2025*)
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT-EE	Computer Emergency Response Team Estonia
CISA	Cybersecurity and Infrastructure Security Agency (USA)
CTF	Capture The Flag (a type of cybersecurity competition)
DigComp	The European Framework of Digital Competences for Citizens
eKool	Estonian school management platform
EdTech	Educational Technology
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
HARNO	Education and Youth Board of Estonia (*Haridus- ja Noorteamet*)
IP	Internet Protocol
IT	Information Technology
IRP	Incident Response Plan
MITRE ATT&CK ®	MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework
MOOC	Massive Open Online Course
MyDigiSkills	A self-assessment tool based on the DigComp framework
NAT	Network Address Translation
Nmap	Network Mapper
OECD	Organisation for Economic Co-operation and Development
PBL	Project-Based Learning
PISA	Programme for International Student Assessment
PPP	Public-Private Partnership
RIA	Information System Authority of Estonia (*Riigi Infosüsteemi Amet*)
SOC	Security Operations Center
SPF	Sender Policy Framework
STEM	Science, Technology, Engineering and Mathematics
TalTech	Tallinn University of Technology
URL	Uniform Resource Locator

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Background

Today's world is driving a shift in the way we learn towards digital technologies. Students communicate and interact with information in a new way, with access to a wide range of educational resources and interactive learning opportunities. When used effectively, this integration improves learning, but along with the benefits, it also brings the risks of cyber threats. These risks include threats to personal data, malware infection, identity spoofing, receiving false information, etc. Moreover, modern hybrid warfare methods on the world stage directly or indirectly affect Estonia's cyberspace [1]. In some European countries, such as Estonia, Ireland and the Netherlands, "schools are not obliged to teach informatics, and/or students can choose whether or not to study it" [2].

The Estonian Cyber Security Strategy 2024-2030 [1] emphasises the importance of integrating cyber security into school curricula, promoting early education and developing a new generation of qualified specialists. In 2018, only one school in Estonia had Cybersecurity included in the curriculum [3]; according to the recommendations [4], the target for 2022 was 20 schools with an elective course in Cybersecurity. Official statistics with up-to-date information could not be found. The vast majority of schools simply lack resources. Initiatives and projects like *e-Koolikott*[5], *Targaltinternetis* [6] and *ProgeTiiger* [7] are emerging to help teachers, students and parents with teaching materials and recommendations on the topic. However, a unified cybersecurity education programme in schools has yet to be created.

1.2 Problem

Together with other countries, Estonia, a leader in digital innovation [8], also faces global issues. However, as a report from the Ministry of Economic Affairs and Communication [1] and research by the CCDCOE [9] show, cybersecurity education in schools remains fragmented, often limited to basic elements of digital literacy. Digital competence looks like a fundamental skill in the modern era. But users often avoid safe online practices. The lack of mandatory cybersecurity education in Estonian schools contributes to this problem by creating differences in student knowledge and preparedness. Although some schools offer elective courses for upper-secondary students in IT fields, such as programming and cybersecurity basics, these programs are unavailable everywhere. This knowledge gap not

only puts the security of personal data at risk but also hinders Estonia's efforts to develop a competent workforce in IT-related fields. According to ENISA, even basic cybersecurity knowledge gives students advantages in the labor market [10].

With the growth of digital infrastructure, the need for standardised and mandatory cybersecurity education is becoming critical. According to a report by PRAXIS, Estonia, along with other countries, is experiencing a cybersecurity labour shortage [3]. McKinsey estimates that "the demand for STEM professionals in Europe and the US, driven by AI and automation, will grow by 17–23% between 2022 and 2030" [11]. According to the World Economic Forum's Future of Jobs Report 2024 [12], cybersecurity is among the five most in-demand skills for 2025–2030. With competencies such as artificial intelligence and big data, technological literacy, creative thinking and agility, cybersecurity skills reflect the growing importance of protection in a digital environment.

Cybersecurity knowledge has become necessary with the increasing use of digital tools in education, work, and everyday life. Solving the problem requires a multidimensional approach, from increasing the number of qualified teachers to revising educational standards. Bringing this issue to the attention of key stakeholders, like the government, educational institutions, and the private sector, can help develop a sustainable digital environment since K-12 (kindergarten through 12th grade) education.

1.3 Purpose

The main objective of this study is to evaluate the landscape of integrating cybersecurity knowledge into school programs from different aspects. The study evaluates existing teaching methods to improve cybersecurity competence by analysing students' knowledge, learning attitudes and behaviours. It will examine how technical, pedagogical, social engineering, cultural and ethical aspects can be combined to improve cybersecurity teaching. In addition, the paper identifies and evaluates the role of programming skills in teaching cybersecurity with a focus on Python exercises. A connection to other related disciplines in the upper-secondary school curriculum for IT students will also be established.

Through hands-on work with 12th-grade students, including a survey, classroom observation, and phishing simulations, the study will offer recommendations for improving teaching approach of teaching cybersecurity in Estonian schools. The findings will contribute to further modifications in the educational process.

1.4 Research Questions and Hypotheses

The hypothesis of this study is that Estonian secondary school students currently lack cybersecurity knowledge due to the absence of compulsory curricula and unequal distribution of resources among schools.

This paper explores one main research question, accompanied by sub-questions across five thematic aspects.

RQ How can cybersecurity competence among high school students be effectively developed in a modern school setting, considering cultural, technical, pedagogical, social engineering, and ethical aspects, using the example of one Estonian school?

Cultural Aspect

SQ1.1 What are high school students' perceptions and attitudes toward cybersecurity, and how do cultural factors influence these views?

SQ1.2 How can cultural values and norms be integrated into cybersecurity education to promote digital safety and literacy?

Technical Aspect

SQ2.1 Which practical programming tasks, using Python as an example, are most effective in building technical skills for cybersecurity?

SQ2.2 How can technical skills be aligned with broader educational goals in the development of cybersecurity competencies?

Social Engineering Aspect

SQ3.1 How do differences in specialised training among high school students affect their awareness of and resilience to social engineering tactics?

SQ3.2 What preventive measures against social engineering can schools effectively implement, and how successful are they?

Pedagogical Aspect

SQ4.1 What organisational, methodological, and motivational barriers arise when integrating cybersecurity education into school curricula?

SQ4.2 How can teaching approaches and strategies enhance students' engagement and understanding of cybersecurity?

Ethical Aspect

SQ5.1 What ethical dilemmas might arise when teaching students about cyber defence techniques and tools?

SQ5.2 How can schools balance teaching technical skills with fostering ethical responsibility in cybersecurity education?

1.5 Overview of the Thesis

The paper's structure is designed to guide from the background and main questions through the research process and results to a set of conclusions and practical recommendations.
The first chapter introduces the topic, explains why it matters, and contextualises the research problem. It also lays out the purpose of the work, the hypothesis, and the key research questions that shaped the study.
The second chapter describes the different methods used to gather information, including expert interviews, a phishing simulation carried out in a school, a student survey, and classroom observations. There's also a literature review that looks at what has already been written and researched about cybersecurity education, helping to place this study within a wider context.
Chapter three discusses the phishing simulation in detail. It explains what was tested, how it was carried out, and what results were seen. This part of the thesis also compares the findings to the original hypothesis and offers recommendations based on what was learned.
The fourth chapter brings together all the information gathered and takes a closer look at what it means. It considers different aspects of the topic—technical, cultural, educational, and ethical—and looks at what students and experts said during interviews. This chapter also includes a discussion about what the results mean in practice, and it ends with several concrete recommendations, including what schools and students can do better, and what could be explored in future research.
The final chapter wraps things up by summarising the most important points and reflecting on what this thesis contributes to the conversation about cybersecurity education in schools.
At the end of the thesis, there are several appendices that provide supporting material. These include full transcripts and notes from expert interviews and examples of interview questions. These materials help to give more depth to the analysis and show how the research was carried out.
Overall, this work aims to support efforts to improve cybersecurity education at the high school level and offer useful insights for teachers, policymakers, and students who are navigating the challenges of the digital world.

2. Method

2.1 Overview of the Object

The object of the study is 12th-grade students of a private Estonian-language secondary school (gymnasium) in the Estonian capital region. In the selected school, at the time of the study, the 12th-grade students of the IT direction (four directions of study in the chosen gymnasium) were taught the courses “Python programming” and “Cybersecurity basics” in parallel. There was an opportunity to interact with IT and non-IT students, get advice, and have interviews with teachers, administration, and cybersecurity experts.

The choice of this group is justified by several factors. Starting secondary school, students have an increased digital activity, including for educational purposes. Along with coming of age, people have more responsibility. They start to make independent decisions, including those related to online behaviour, and to take responsibility for the consequences.

Many school graduates are interested in careers in IT and cybersecurity (often due to the high salaries in the field), which highlights the importance of acquiring the relevant knowledge and skills. In addition, public schools are more open to cooperation due to the simplicity of administrative processes.

2.2 Organisation and Conducting Expert Interviews

As part of the empirical section, expert opinions were collected through five semi-structured interviews (conducted via videoconference) and one structured interview in a written form. Interviews with the Head of the gymnasium and two teachers of 12th-grade students in the IT-focused curriculum (teaching Fundamentals of Cybersecurity and Python Programming) were scheduled in advance.

The search and selection of cybersecurity experts from the private sector was facilitated by a cybersecurity teacher who provided references and contact information for potential participants. Six of them expressed willingness to participate; however, due to their heavy professional workload, it was possible to organise interviews with only three specialists. Due to a tight work schedule, one provided written responses to pre-formulated questions. As a result, six expert opinions were included in the study:

- three from cybersecurity professionals;
- two teachers from the gymnasium;
- one of the gymnasium administration.

All participants received a list of questions in advance; during the video conversations, follow-up and clarifying questions were asked, which enabled deeper exploration of the research topics. The questions for cybersecurity specialists were entirely identical. The two 12th-grade teachers were asked partially overlapping questions, while the gymnasium head was interviewed on general research-related topics.

The video interviews were conducted via Microsoft Teams and lasted 30–40 minutes. Respondents agreed on the use of an automated transcript in the interviews. Depending on the content of the conversation, a transcript or interview protocol was prepared and then agreed upon with each respondent. Participants agreed on the acceptable form of mentioning their participation in the study and citing their statements in the thesis. The information obtained through interviews allows previously unknown details to be revealed and expert perspectives to be compared, facilitating a more in-depth analysis of the research topics.

2.3 Overview of the Phishing Campaign

The phishing campaign was designed as an accessible test of 12th-grade phishing awareness and click activity. It also tested the correlation of simulation results between non-IT profiles and an IT profile that had mastered the cybersecurity course. Based on the simulation results, it was possible to make recommendations to school management, students, and technical staff. The simulation was conducted with the permission of the school administration, with the notification of the technical staff, and without the involvement of third parties. The phishing simulation is discussed in more detail in the Chapter 3.

2.4 Overview of the Student Survey

The study originally planned to survey 12th-grade IT students to gather feedback on their experiences, awareness, and attitudes towards cybersecurity. The original plan included a Google Forms questionnaire with 10-15 structured questions. However, the number of questions was reduced during the research process because of theoretical research and expert responses. Therefore, the data collection method changed to an email survey distributed through the cybersecurity teacher. The teacher sends answers back to the

researcher without names.

Students were informed that their responses would be anonymised and used strictly for research. The sample group consisted of 16 students from a core IT class, and participation in the survey was entirely voluntary. The enquiry was made during the period of state examinations, so the number of responses was limited. Nevertheless, the feedback received provided some insights. Details of the results are analysed and discussed in more detail in Section 4.2.1.

2.5 Classroom Observation Overview

A classroom observation was conducted in April 2025 at the private school under study in this research. The observed group consisted of 12th-grade IT students who were attending their last cybersecurity lesson of the course. Eight students were present; the rest were absent due to a valid reason (a study event). The purpose of the classroom observation was to understand the level of student involvement and role in the lesson, and to study the method of conducting the lesson.

During the lesson, students presented their final projects in the form of a significant incident analysis. The structure required them to explain what happened, who was harmed by the incident, why it mattered, and how it could have been prevented, in a volume of about 5 slides. The presentations were structured and done without apparent technical difficulties – students connected their devices and used the projector independently. The teacher asked a question after some presentations or explained small details, but the main activity was from the students.

This format reflected a flipped classroom approach, where students prepared content in advance and presented their work in class. The overall atmosphere was positive, but some students were a little nervous when presenting. The students listened to the presenter's story but did not ask questions. A couple of presentations were hastily done, with a black and white background or much text on the slide and information being read out loud. Most presentations were professionally designed and even wow-inducing in their structure and design. In conclusion, the teacher thanked everyone and discussed a few more points on the lesson topic. The course assessment system was pass or fail. Students who were absent from the lesson presented their project at a separately agreed-upon time.

Observation has shown that having students solve real-world problems, such as presenting cybersecurity incidents, helps them apply technical knowledge while developing critical thinking and public speaking skills. Approaches such as project-based learning and the

flipped classroom model make technical content more meaningful by linking it to broader digital competency goals, such as those outlined in DigComp 2.2.

2.6 Literature Review

This literature review examines existing research, frameworks, and national strategies that inform cybersecurity education at the upper secondary school level. The review is based on key themes: international and national frameworks, teaching methodologies, ethical and pedagogical challenges, and current Estonian initiatives and tools. Theoretical Framework

According to ENISA [13], cybersecurity education should be introduced early to create a sustainable digital society and is the main priority in the educational roadmap. The report [10] notes that reviewing educational and training programs in Europe is needed to address cybersecurity education and training challenges. The challenges include a lack of ability to motivate students to choose academic fields related to cybersecurity and to prepare professionals with the necessary knowledge and skills.

ENISA [13] has a mandate to support cybersecurity in member countries and raise public awareness, including cyber hygiene and cyber literacy, at all levels of education. The European Commission's DigComp 2.2 framework [14] defines digital security as one of five core competence areas, including information literacy, communication, content creation, and problem solving.

Talent acquisition and development is an important topic for the labour market in the fast-growing cybersecurity industry. There are such competitions for youth in Estonia, like Cyber Battle by CybExer Technologies [15], CyberDrill [16] or CyberSpike [17]. According to research [18], while CyberCracker (for 12-15 year-olds) is helpful for talent discovery, it falls short in supporting talent development.

2.7 Theoretical Framework

Current approaches to teaching cybersecurity can include project-based learning (PBL) and the flipped classroom model. These have a positive impact on lesson engagement, and students perform significantly better academically than in traditional instruction, especially for STEM subjects [19]. However, this PBL approach may also require extra effort from technology teachers when applying new approaches and taking into account the results of their work to improve the methodology [20].

The research also relies on the DigiComp 2.2 Framework, especially areas 2, 4 and 5 - Communication and Collaboration, Safety and Problem solving. The author points to the multidimensional approach of the study as the theoretical framework. This implies looking at the study of cybersecurity education through ethical, cultural, technical, pedagogical and social engineering lenses.

3. Phishing Simulation in a School Environment: Analysis and Findings

3.1 Introduction

This master's thesis presents a phishing simulation conducted in a secondary school (gymnasium). The goal was to evaluate the awareness of 12th-grade students about cyber threats (especially social engineering) and assess the effectiveness of cybersecurity education among IT and non-IT study profiles. The simulation helped identify technical and psychological factors influencing students' susceptibility to digital deception and discovered areas for improvement.

3.2 Hypotheses

The phishing simulation part of the research focused on three central hypotheses.

Hypothesis 1: Students from the IT profile who have received a cybersecurity course will demonstrate higher resistance to phishing attacks than their peers in other study profiles. IT students are more familiar with phishing, can verify sender addresses and URLs, and are more likely to recognise social engineering techniques.

Hypothesis 2: Phishing emails written politely and trustworthy about school-related topics will lead to a high engagement rate and click-through behaviour. Students are inclined to trust content that appears to be part of school life, especially if it is written shortly, does not require much time for action, and is received during school hours.

Hypothesis 3: Most clicks on phishing links will occur within the first hours after receiving the emails. Students tend to check their school mailboxes in the morning or during breaks. Additionally, once suspicions arise, information may quickly spread through internal communication channels such as class chats or orally during a school day, suppressing further click activity.

3.3 Methodology

The phishing scenario was developed based on on-site observations at the school and analysis of student interests and communication patterns. Two themes were chosen: voting for participants in a music competition (Figure 1) and evaluating the quality of school meals (Figure 2). These were considered emotionally neutral but engaging topics. Emails were written in Estonian, using polite and natural language to enhance realism.

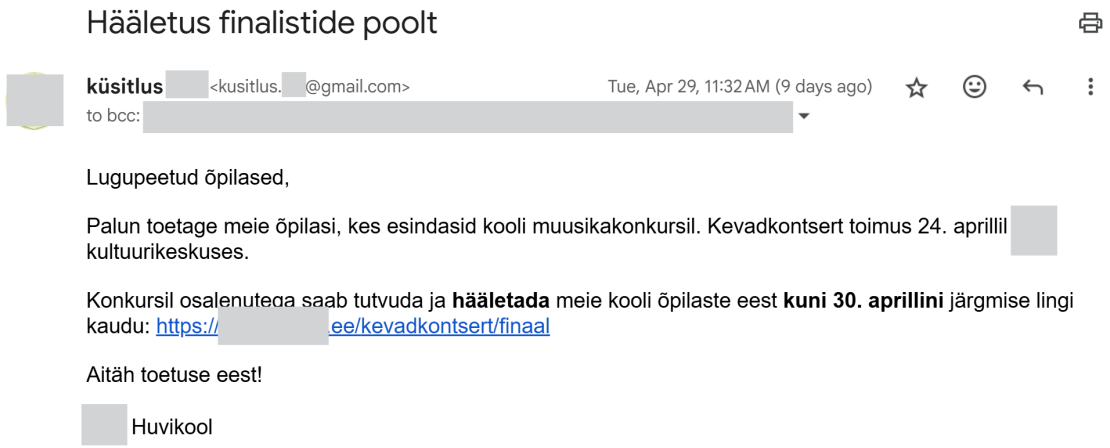

Figure 1. Phishing simulation. Voting invitation email sent by a hobby school department (in Estonian).

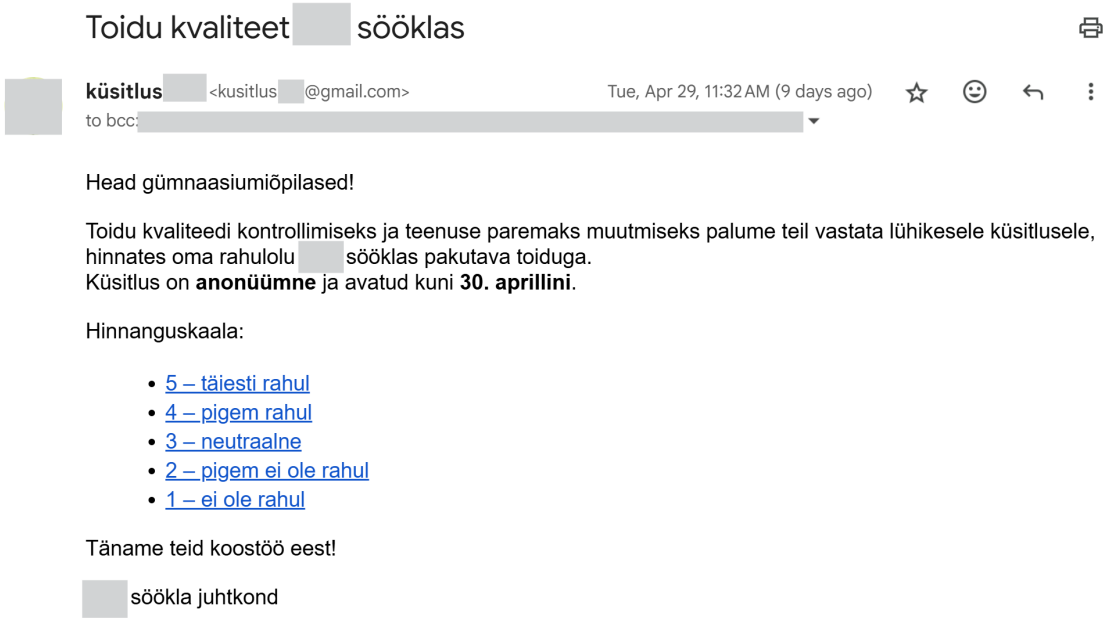

Figure 2. Phishing simulation. Email survey about food quality sent by the school canteen management (in Estonian).

The researcher created a special Gmail account under the name “Survey.SchoolName” (in Estonian) with the logo confirming school affiliation. However, the domain was a regular Gmail domain, not a school domain.

The Canary Tokens tool [21] was chosen as the marker for click counts. A review of the terms and conditions associated with Canary Tokens has confirmed that user data will not be sold or shared, ensuring that the simulator is ethical [21]. It should be noted that Canary tokens do not violate privacy laws as they do not collect personal user data, making them a legitimate tool for security tests and catching attackers. In the case of such a mass mailing, it is impossible to identify the students who were clicked because Canary Tokens does not extract names, logins, or similar sensitive data. Identification is only possible if a unique token is sent to a specific person.

A Web bug type of tokens, which were redirected when a page was clicked, was chosen for testing. The page that opened had a globe spinning, and the page address started with the words “canary tokens”, which could immediately arouse suspicion. Therefore, other selected tokens were tested, and a token with the “Fast Redirect” type was chosen. These redirected users to legitimate external websites (the school’s official page or the cultural centre where various concerts are conducted) without the user noticing any suspicious details. Four unique tokens were used, each tied to one of the combinations of student profile and scenario: Canteen food IT, Canteen food non-IT, Final voting IT, and Final voting non-IT. These designations enabled the researcher to identify the specific group to which the clicks belonged. The click data comprised the token label, external IP address, timestamp, and User Agent description, all of which were automatically emailed to the researcher.

3.4 Implementation

The simulation was conducted with approval from the school administration and the system administrator. The estimation of results lasted for 48 hours. Messages were sent to students’ addresses provided by the school administration. Email addresses were randomly selected across four classes. The 12th-grade email list included 66 students, 16 of whom are in the IT profile. Each of the 4 classes received 5 emails for the two email scenarios. A total of 40 emails were distributed, two of which bounced due to inactive accounts (from a non-IT email list). Administration has confirmed that 2 accounts are inactive and can be removed from the simulation. Thus, 38 of the 64 12th-grade students received letters from the researcher: 10 to the IT-profile group and 28 to the non-IT groups.

The first email text was sent on behalf of a hobby school. The email asked the students

to support the school's students participating in a music competition at one of the city's cultural centres and vote for them via the provided link. The second text is an email allegedly sent from the school cafeteria administration. It asks the students to rate from 1 to 5 the quality of the food, offering to take an anonymous vote. Each rate is the same link for counting clicks. Both emails redirected to the corresponding home pages - the school or cultural centre website - but no voting appeared on the screen. Both emails imply a deadline, which puts pressure on the receivers. Visually, the emails look credible and official, which makes them trustworthy for the students. These emails were used in a phishing simulation to assess the students' awareness.

To be more ethical, the simulation avoided emotionally sensitive topics such as final exams and was limited in the scope of the mailing. A wider campaign using an external domain would likely have aroused suspicion and led to disruption.

3.5 Results

Of the 38 functioning addresses, the IT profile had 2 clicks (20%), and non-IT had 19 out of 28 (approx. 67.9%) (Figure 3). Most activity occurred in the first hours following distribution (Figure 4). Clicks significantly dropped afterwards, potentially due to peer discussion and warnings shared through school communication tools.

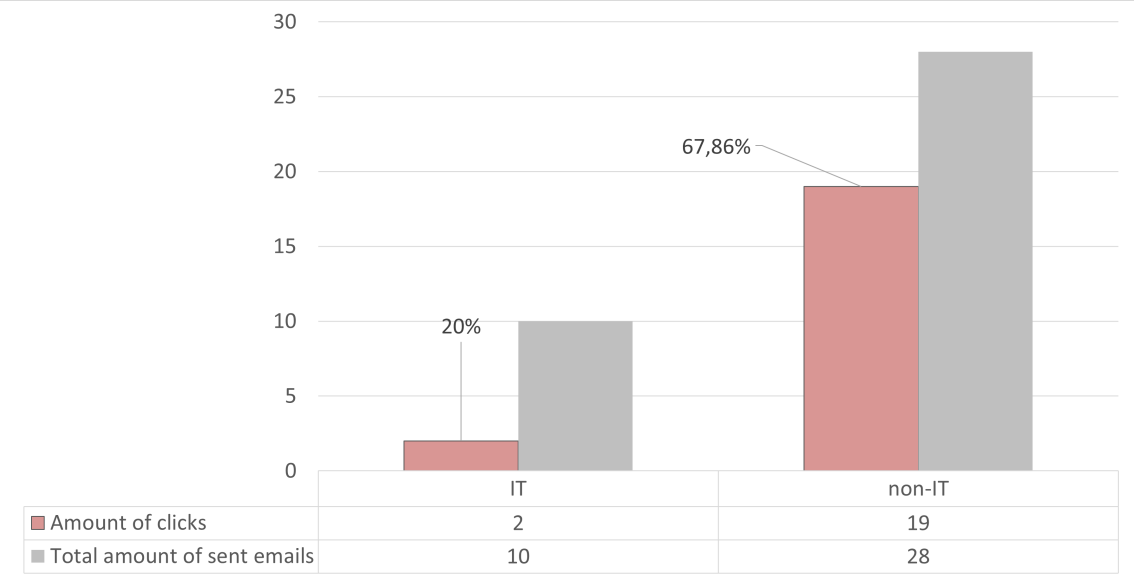

Figure 3. Comparison of clicks on phishing emails in IT vs. non-IT groups

Canary Tokens logged external IP addresses and User Agent descriptions. Some IPs and agents repeated, indicating the school's Network Address Translation (NAT) usage. The

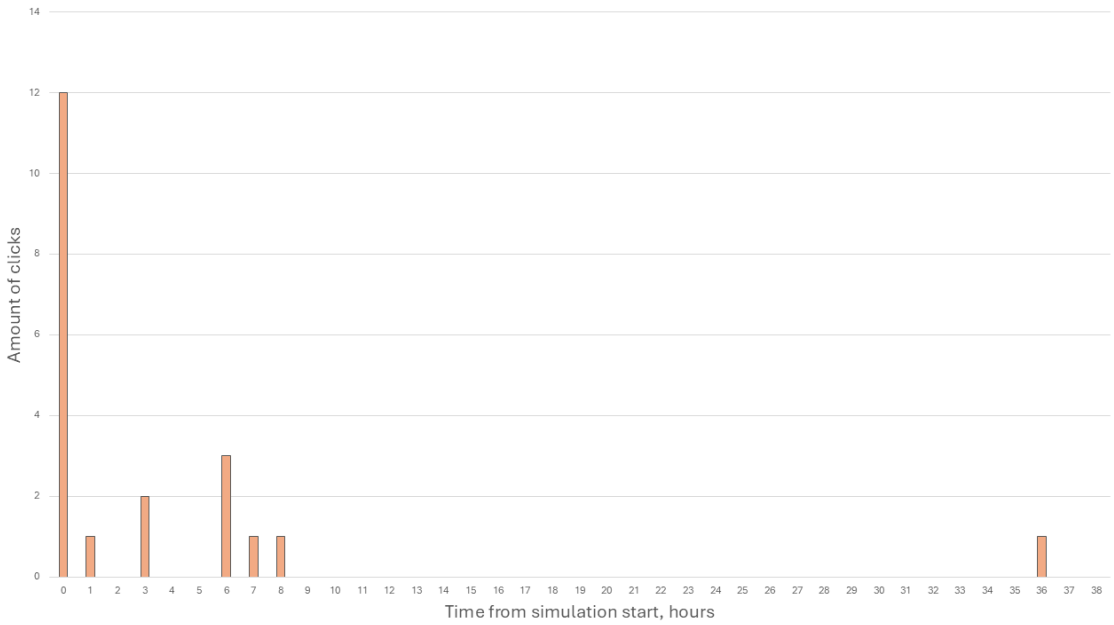

Figure 4. Click activity over time since start of phishing simulation

administration confirmed that NAT was in place, meaning multiple users could appear under the same IP. For example, one IP address had three clicks within four minutes, and another had two clicks hours apart. These may reflect different users or one person re-clicking.

Even accounting for repeated clicks when sending to non-IT profile students, there were at least 16 unique external IP addresses, so the number of unique clicks is 16 out of 28 (approximately 57%). It can also be assumed that one of the students clicked from a school computer and then came home and opened the link from a mobile phone. In this case, the external IP addresses would be different, and the user could have made several clicks from different devices. This study does not state that one click equals one user being phished. Summarising the overall results of the phishing simulation in grade 12, it can be noted that out of 38 emails sent out, there were 21 clicks (55.26%). Considering clicks only from unique external IP addresses, 18 out of 38 emails were sent (47.37%).

Analysing the User Agent type of all results revealed that 7 clicks were made from desktop devices and 12 from mobile devices (iPhone or Android). Another 2 clicks could not be categorised clearly, as their User Agent contain "Google-Firebase" information, which does not allow to determine the device type.

Among the factors that influenced the number of clicks are the following:

– Persuasive and well-formatted email content in the Estonian language

- The timing of delivery during school hours enhanced trust and increased the likelihood of reading.
- Insufficient attention to sender information or thorough URL examination.
- Strong connections within the school community and a desire to support school initiatives.
- Limited familiarity with external emails and a general lack of awareness regarding phishing threats.
- Use of mobile devices instead of desktop devices.
- In IT classes, curiosity and recognition of the Canary Token may have encouraged exploration rather than eliciting fear.
- Conversations with classmates in chat rooms could diminish or halt clicking behaviours.

3.6 Response to Hypotheses

The results support all three hypotheses:
1. This significant difference (IT-direction 20% compared to non-IT 67.9%) indicates that prior exposure to cybersecurity education had a measurable impact on students' ability to recognise and avoid phishing attempts. Furthermore, some IT students may have clicked on the link intentionally. Given previous lessons on Canary tokens and social engineering, they might have noticed the URL that indicated it was a Canary token and opened it for interest.
2. The emails used in the simulation were written in Estonian clearly and politely. They addressed relevant and emotionally neutral school-related topics such as voting for peers or evaluating school canteen food. Both groups were more likely to click on "Final Vote" than "Food in the Canteen", but the difference is not highly visible due to the small sample of letter recipients (Figure 5).
These messages required only a few clicks and did not demand significant effort. Such characteristics likely increased the trustworthiness of the emails and contributed to the relatively high click rate among non-IT students. The emotional proximity and simplicity of the messages played a significant role in encouraging user interaction, as evidenced by the high click-through rate.
3. Most clicks occurred within the initial hours after the emails were sent (see the Figure 4). Click activity stopped almost entirely after the first few hours of the simulation. This decrease can be attributed to in-person communication and messaging through class chats, where students probably alerted each other to the suspicious nature of the emails. This pattern underscores the importance of social interaction and the quick dissemination of insider information in mitigating the spread of phishing threats.

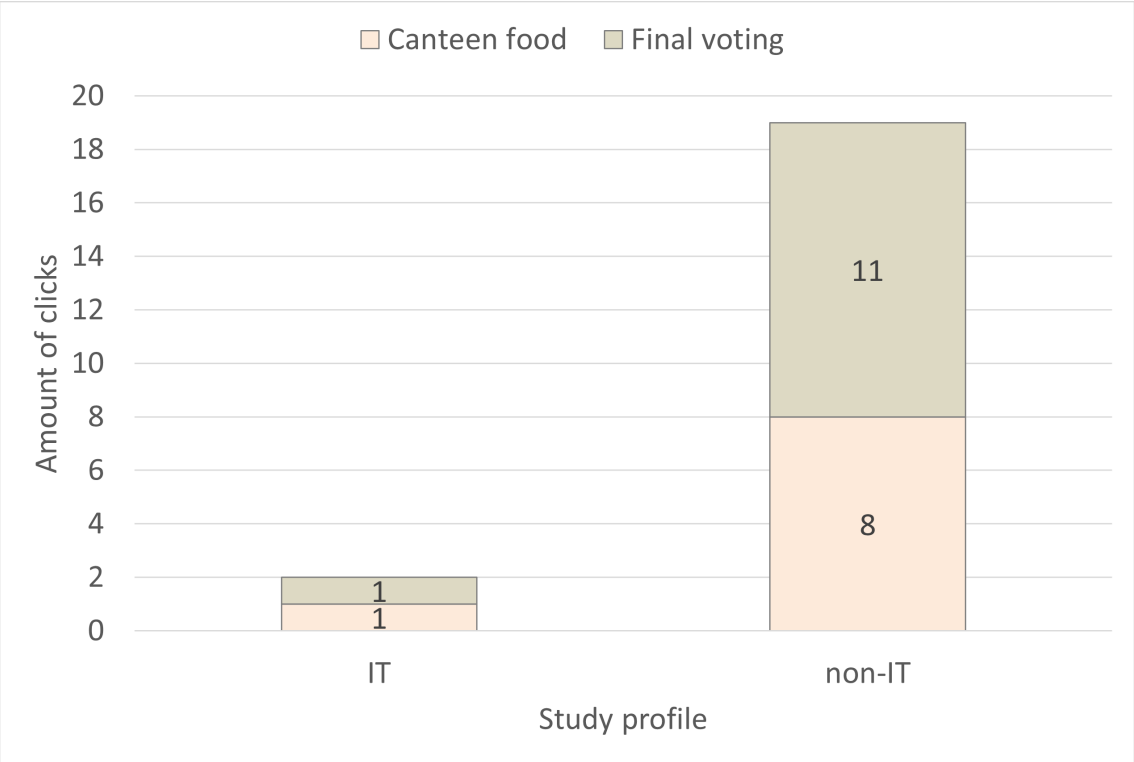

Figure 5. Number of clicks on phishing emails with different subjects, grouped by study profile

3.7 Conclusions and Recommendations

Users on mobile devices are particularly vulnerable to phishing attacks due to their limited options for verifying links. Whereas desktop users can hover over the URL, mobile users must take additional steps, such as long pressing to verify a link (which many people do not do). This behavioural limitation enhances the effectiveness of phishing attempts. In the simulation context, it clarifies why even well-trained students might have clicked on malicious links, as they were accessing the email on a smartphone instead of a desktop.

As the school principal responded, there have been no major incidents at the school yet, and the cybersecurity subject is being taught for the first year (Appendix 8). The relatively high percentage of clicks may be related to the phishing simulation precedent.
The following conclusions and recommendations will be offered:

- The simulation results show that a Cybersecurity course and IT direction in the gymnasium significantly improve resilience to phishing attacks.
- Social context matters: trust and cohesion among students can increase vulnerability and facilitate rapid defence once suspicions arise.
- Cyber awareness principles should be introduced to all students, regardless of their

study profile. Key practices should be reinforced annually.
- Implement technical safeguards, such as banners on external emails warning: “This email is from outside your school. Be cautious.”
- To follow up, a general summary email with anonymised results and reminders to remain attentive was sent to all 12th-grade students. School administration may adapt this message for other classes.
- Similar simulations could be extended to include school staff in future training initiatives.
- The full simulation results were forwarded to the school’s system administrator for further analysis and improvement by the school.

According to the study’s findings [22], warnings on emails are indeed effective in preventing the effects of phishing and built-in training during a phishing simulation, as is done these days, can make users even more susceptible to phishing. In other words, training should be systemic and preventative, not as a consequence of phishing simulations. Thus, phishing simulations are practical tools for raising awareness and identifying areas where targeted educational and technical interventions are needed.

4. Analysis, Discussion, Conclusion

4.1 Analysis

4.1.1 Cultural Aspect

The study's cultural aspect is closely linked to Estonia's nationwide drive towards digitalisation and innovation, which shapes young people's awareness of the importance of IT and cybersecurity in modern society. Starting in the 1990s, Estonia made a strategic choice in favour of information technology (IT) development, which led to the formation of an advanced e-society and e-state [23]. Since 1996, all schools have been provided with internet access, which is related to the now famous Tiger Leap (*Tiigrihüpe*) programme in Estonia [24].

Estonia has become known as "e-Estonia", a country with one of the most developed digital ecosystems in the world [25]. The daily habit of using electronic services creates a false sense of safety in cyberspace. The population, including high school students, should be raised to awareness of cyber risks. Attention to cybersecurity is publicised in society through social advertising and television. Service providers' websites, such as delivery services (Figure 6) or banks, constantly warn users about increased fraud.

Figure 6. Omniva's cybersecurity notice to users. A public warning against phishing on the website of Estonia's national postal operator.

From December 2024, all the government services in Estonia are available online [25], making it much easier for citizens to interact with the State. As a result of the favourable environment for innovation, Estonia has spawned many IT startups, and the country leads Europe in the number of "unicorns" (companies with a valuation of more than $1 billion per capita) [26]. These companies include Skype, Bolt, Wise, Pipedrive and others [26]. The IT sector has become popular among Estonian youth, attracting talent and contributing

to the development of the digital economy. Programmes such as *ProgeTiiger* [7] aim to increase technological literacy from an early age, helping to create a new generation of IT professionals.

Various local activities are carried out in EU countries to teach children and adolescents about cybersecurity. For example, in Austria, France, and Portugal, lessons or modules on cybersecurity are introduced, and various challenges and hackathons are held [13]. In Estonia, with the support of the Ministry of Education, the Tallinn University of Technology is developing a program for schools. However, measuring the impact of initiatives on the target audience is a task that Member States are trying to solve [27].

In February 2025, Estonia's Ministry of Education and Research announced a new education programme, AI Leap 2025 (*TI-Hüpe 2025*) [28, 29]. Artificial intelligence is forming a new era in education, widening access to knowledge for students and teachers.

4.1.2 Technical Aspect

Considering the issue of linking programming with other subjects, it can be noted that students are usually more motivated to learn the subject and more interested in and understand the course of tasks and exercises if the result of actions is tangible. It was noted in a Swedish study that simple text programming in Python seemed boring to secondary school students until teachers linked it to Maths or Technology [30].

However, in the interview (see Appendix 7), it was noted that extra time was spent on installing virtual machines before the lab in the cybersecurity lessons. Difficulties arose due to some students' lack of technical skills and different operating systems, when using school or personal computers. According to the teacher, more advanced students helped their classmates, reflecting their good team spirit. The lessons included teamwork, the implementation of PBL in solving programming problems and cybersecurity labs, and developing digital competencies (DigComp 2.2.)

4.1.3 Social Engineering Aspect

This section addresses SQ3.1 and SQ3.2. Phishing, as the object of the technical practical part of the study, was chosen as one of the most common and easily reproducible types of social engineering. Its relevance is due to the widespread prevalence of cybercrime at school in real practice and significant educational potential in developing elementary digital hygiene skills in students [31], [32]. According to the MITRE ATT&CK® knowledge

base [33], phishing is one of the techniques for the initial access tactic. These techniques may also be used in later stages of incidents [27]. The report [34] shows that in Estonia, in 2024, 65 % of all incidents with consequences are phishing. The use of phishing for educational purposes not only to clearly illustrate the mechanisms of cyberattacks but also to develop critical thinking in schoolchildren, the ability to analyze the information received and recognize potential threats. K–12 institutions are prime targets due to their access to sensitive student data [31].

The topic of phishing covered in cybersecurity lessons and the general technical knowledge of students in the IT direction likely them to be more successful in recognising suspicious elements in an email. The success of the simulated phishing campaigns demonstrates how schools can effectively integrate low-risk, high-impact social engineering exercises (SQ3.2). They help students understand emotional triggers (urgency, authority, desire to support), consistent with broader digital hygiene goals. Among other measures to SQ3.2, the Cybersecurity teacher (in person, after interview) suggested role-play days (scammer vs. victim), reflecting with students on ethical issues and attackers' goals.

4.1.4 Pedagogical Aspect

According to the PISA 2022 report, Estonian students aged 15 performed above the OECD average in mathematics, reading, and science [35]. In 2018, Estonia's performance was ranked 1st in Europe [36]. According to the Cybersecurity Strategy 2024–2030, cyber hygiene and cybersecurity will be included in school curricula by the end of 2027 [1]. As a school representative (Appendix 8) meant in an interview, IT-related skills should be woven into other subjects, which is much more effective than teaching it as a separate subject. However, according to the report [2], for 2020/2021, less than half of European countries have integrated computer science into high school alongside other subjects. Mostly, these were optional subjects or specialised studies in upper grades (i.e., some subjects are compulsory only for specific profiles).

Organisational barriers include the teacher national shortage, the lack of cybersecurity teachers (here comments from the gymnasium director), and the need to find them in the private sector. The lack of teachers, methodological and technical resources in the school is also noted in other reports [7], [13]. In terms of methodological barriers, as noted by the Cybersecurity teacher (Appendix 7), there were no serious barriers except for a huge amount of different materials to choose from. Among the motivational barriers, it is also worth noting the general condition of graduating students before exams and their workload and anxiety. It can be assumed that the cybersecurity elective course can be taught a couple of classes earlier, or the course can be divided into short modules and gradually learned

over several years. Data from interviews (Appendix 7) confirm that tasks related to real-life situations, such as creating a password checker and a Canary token lab, increase student engagement and understanding.

4.1.5 Ethical Aspect

The Gymnasium State Curriculum aims, among other things, to develop ethically responsible individuals with digital competence to effectively use technology and innovation in a rapidly changing world [37].

According to the cyber teacher's answers (Appendix 7), the topic of ethics was mentioned in the lessons, but a detailed discussion of ethical issues requires more class hours. One of the homework assignments was to prepare a presentation on any major cyber incident with an analysis of the consequences and a proposal for protective measures. Cyber protection and cyber awareness also cover the topic of hacking. If students gain knowledge about hacking tools, as password checkers or practical tools of social engineering (Appendix 7), then awareness of responsibilities should be covered equally.

The ethical component of life in cyberspace should also be covered to ensure the correct use of artificial intelligence by high school students. Using real-life examples to discuss ethical dilemmas helps students identify legal and illegal actions. Incorporating ethical reflections into each practical (technical) task will help strengthen responsible behaviour as a digital citizen.

4.2 Discussion

4.2.1 Student Feedback Analysis

Table 1 compares the students' anonymised feedback on the same questions. 3 out of 16 students responded to the voluntary email survey, but even this small sample provides some feedback on cybersecurity awareness and training in the school. Overall, students noted that they can help others, some became more technically aware after the course, and others changed their online behaviour and password culture. Among the useful topics to study were digital reputation, online ethical behaviour, data protection, and ways to recognise social engineering. Among the more useful methods, all students tend to choose practical cases and group work, as well as independent study, along with information provided by an expert teacher.

Table 1. Student Interview Responses on Cybersecurity Topics

Question	**Student 1**	**Student 2**	**Student 3**
Have you or any of your friends ever experienced a negative incident online? If yes, how did you respond?	No personal incidents; very careful online.	Friend's social media hacked via phishing; helped recover account, reported it, changed passwords.	Yes; informed the person whose account was compromised.
Do you discuss digital safety or online risks with your parents or relatives? Do you share what you've learned with them?	Yes, a lot. Main points: avoid posting face, unknown links, calls; strong passwords; limit sharing personal info.	Sometimes, especially when scams appear; explains fake info and password importance.	No, very rarely.
Has your online behaviour changed after the school cybersecurity course?	Not much changed, already followed safe practices; gained deeper understanding of why.	Yes, definitely; started using 2FA, verifying websites, mindful of shared info.	Yes; more attention to strong passwords.
Which topics are the most important to include in a school cybersecurity course?	Real-life skills, especially for non-IT students; caution with QR codes and suspicious emails.	Data protection, phishing, digital reputation, online ethics.	Data protection, phishing, strong passwords.
Which learning methods do you find the most interesting and helpful when studying new topics?	Projects requiring effort; prefers lectures from passionate experts; needs theory before practice.	Practical case studies, role-playing, group projects for peer learning.	Practical tasks, self-research alongside teacher guidance.

4.2.2 Analysis of Cybersecurity Experts Interviews

Table 2 compares the experts' opinions on the same questions (see Appendix 2). Full interview protocols or transcripts with Expert A (see Appendix 3), Expert B (Appendix 4) and Expert C (Appendix 5) are in the appendix. Experts agree that the situation on the labour market is critical. Sometimes it is necessary to attract employees from abroad. Expert C (Appendix 5) noted that the shortage is especially felt at subsequent career levels, not entry-level positions. Expert B (Appendix 4) indicated that the awareness of cybersecurity among young people is at different levels. Expert A (Appendix 3) believes that phishing simulation is overrated, but together with staff training, it is a working tool. Expert B supports this method, together with training and cyclical training.

The experts also noted the difference in understanding the business context, highlighting the importance of internships and onboarding. One expert expressed the opinion that within six months it is possible to learn applied skills, having a good theoretical base. Another said that it is possible to come to cybersecurity with an education in another speciality; it all depends on the position. After interviewing three experts, it can be concluded that

Table 2. Comparison of Expert Opinions on Cybersecurity Education for Youth

No.	EXPERT A	EXPERT B	EXPERT C
1	Does not evaluate school graduates; mentions talent shortage, awareness varies.	Distinguishes enthusiasts from overconfident novices; the onboarding process is crucial.	Rarely works with youth; confirms shortage in the second and third lines of defence.
2	Emphasises awareness and 'healthy paranoia', rational thinking.	Awareness through simulations, red flag detection, caution.	Resilience under pressure is key.
3	Phishing simulations are overrated, practical training is needed.	Simulations useful if repeated and supported by technical controls.	Simulations and training help, but full protection is impossible.
4	Mentorship and practice are crucial; notes lack of legal awareness among students.	Gaps in corporate practices and technical basics; basic knowledge of programming is required.	Governance is undervalued in education; does not comment on schools.
5	Actively collaborates, gives guest lectures, willing to share experience.	Sees potential for collaboration but lacks time to participate.	Has past collaboration experience; does not mention teaching readiness.
6	Theory + practice; insists on deep, hands-on training and attack demonstrations.	Prefers interactive, concise training, simulations, hands-on experience.	Balanced approach needed, adapted to audience psychology.
7	Very important; technical skills and ethics must be taught together.	Fairly important; explains legal boundaries and accountability.	Ethics should be basic; AI ethics still immature, open discussions needed.
8	Technical training should be strong; train specialists to the best of their ability.	Legal clarity and consequences are essential; personal responsibility matters.	Like med/law schools: skills can be misused; must stay within legal limits.
9	Promotes the field as profitable and socially meaningful.	Stresses specialisation, goals, and risk-based thinking.	Think that value formation happens earlier than in high school.
10	Supports AI integration in schools, mandatory informatics, and guest lectures.	Cyber hygiene basics for all; teachers should motivate, offer extra activities.	Emphasises governance, leadership support, asset/config management, and business context.

mostly young specialists come after university. Ethics training is considered important, but it is often a person's view of morality. Among the effective methods, experts support interactivity, but it is also necessary to take into account and understand the psychology of people. The experts interviewed have different experiences and specific work activities, which also influence the various degrees of their interaction with young people.

4.2.3 Analysis of Education Expert and Teachers Interviews

This chapter examines the responses to interviews with education experts. The author asks the experts about their experiences, views on education, and specific subjects such as programming and cybersecurity. Topics such as challenges in teaching, curriculum content, student motivation, the role of technology (particularly artificial intelligence), ethical aspects, and general questions regarding the organisation of school life and the education system in Estonia are discussed.

The study included interviews with three experts representing different sides of the educational process: the programming teacher (in Appendix 6), the cybersecurity teacher (in Appendix 7) and the high school principal (in Appendix 8). Their opinions helped identify everyday teaching problems and global issues in teaching IT disciplines in the school environment. The interviews confirmed that teaching programming and cybersecurity in high school intersects with traditional teaching methods and new challenges of the digital age. Teachers named different levels of preparedness and motivation for the specific problems. They all noted the risks of thoughtless use of AI and the risk of abandoning independent thinking. All three experts emphasised the shortage of personnel as one of the serious problems for the education system.

Teachers must adapt to a diverse audience and adjust expectations and course pacing to the specific class. This requires flexibility and pedagogical skill, which can sometimes lead to frustration, especially if students are not interested in and unwilling to work independently.

One of the new but already noticeable challenges was the influence of artificial intelligence, primarily accessible tools like Chat GPT and Gemini. All three experts expressed concern that students increasingly try to delegate tasks to AI without delving into the essence. This reduces the quality of education because the main goal is to learn to think, not just hand in a ready-made solution. The school principal highlighted this problem especially acutely, emphasising that "outsourcing of thinking" seriously threatens the school's educational mission (Appendix 8). In this regard, he believes classic homework is losing its relevance in some subjects (especially STEM) and requires revision. The ethical side of teaching IT subjects was also discussed. Teachers acknowledge that any skills and knowledge can be

used for good or for harm. Therefore, it is important not only to teach technical skills, but also to discuss ethics, legal implications and personal responsibility from the beginning. Although the school does not have a formal digital ethics code, these issues are raised in dialogue and internal workshops for teachers.

All three experts also pointed to a systemic problem — a shortage of qualified teachers. In conditions of high competition between schools and the lack of a constant influx of young specialists, this problem is becoming acute. Additional reserves can be attracted from the industry, for example, specialists who are ready to take on a useful social load and have sufficient qualifications. According to the school director (Appendix 8), it is necessary to improve the image of teachers and make the profession more respected in order to attract new specialists.

The experts demonstrated a unified desire to update the content and teaching methods. They all noted that IT disciplines should be as practice-oriented as possible. Examples of the practical part include ethical hacking on Kali Linux, working with cloud labs such as TryHackMe and Hack The Box, and participating in CTF competitions (Appendix 7). This helps students not only remember information but also feel connected to the real industry. Using the interdisciplinary approach, teachers coordinate topics between programming and cybersecurity courses so students can see the big picture, such as how encryption theory is applied in code.

The director generally supports integrating digital literacy into various subjects, including math and science, rather than creating isolated courses (Appendix 8). Particular attention is paid to developing "soft skills" — critical thinking, learning, working in a team, and adapting to new things. Teachers consider these qualities to be as important as technical skills. Programming teacher links motivation and willingness to learn with "enjoyment" from the process (Appendix 6), which is becoming an integral part of the pedagogical philosophy. Public-private partnerships strengthen the school's links with the outside world and make learning dynamic.

To improve the educational process in schools, feedback should be collected from students and teachers. All three experts agree that IT education requires new approaches that are flexible, practical, ethically sound, and open to collaboration. At the same time, there are several significant challenges: a shortage of teachers, varying levels of student preparedness, and the necessity to adapt to new technologies.

The analysed experience of the studied school can serve as an example of teaching cybersecurity in the gymnasium. Interviews with teachers confirmed that technical competence

and pedagogical flexibility accompany strategic thinking. Student engagement is directly related to the practical applicability of knowledge, the quality of interaction with the teacher, and the opportunity for self-realisation. In the context of rapid technological development and the introduction of AI, traditional approaches are losing their effectiveness, which requires schools to develop innovative solutions and dare to change.

4.3 Recommendations

4.3.1 Recommendations for Policymakers and Schools

Public-private partnership (PPP) has been successfully used in Estonia for several decades [23]. The private sector helps develop infrastructure and technology, for example, in energy (Enefit Green [38]), construction (Rail Baltica [39]) and educational innovation (eKool [40]). Praxis policy brief emphasises the importance of PPP in promoting digital education in the Baltic States[41]. The CISA report [31] emphasises the importance of the partnership between the private sector and K-12 and the development of an incident response plan (IRP). The Estonian state should support programs such as Startup Estonia's EdTech, which promotes cooperation between startups and educational institutions. In particular, PPP is relevant, especially when teaching elective subjects in upper secondary schools. Involving the private sector in education provides students with relevant and practical knowledge. As a result of this partnership, the private sector will face questions and challenges from a generation of future professionals, giving it new ideas for development/

In addition to teaching students about cybersecurity, school staff should also be mentioned. For example, the Estonian Information System Authority (*Riigi Infosüsteemi Amet*, RIA) plans to inspect state high schools, public universities, and possibly some municipal schools in 2025 [32]. To increase staff cyber awareness, taking the RIA Cyber Test [42] is also suggested, which includes training and testing parts. RIA experts note that "the level of cybersecurity in a school depends on the management's attitude to data protection and the safe use of digital tools" [32].

4.3.2 Recommendations for Students

This section provides the author's recommendations for high school students in Estonia. Many of the recommendations also apply to the education process as a whole. High school students can prepare themselves smoothly for entering the labour market by examining the skills a modern digital citizen needs, such as those outlined in DigComp. The MyDigiSkills tool [43] enables students to self-assess their skills for free and identify areas

for improvement (Figure 7).

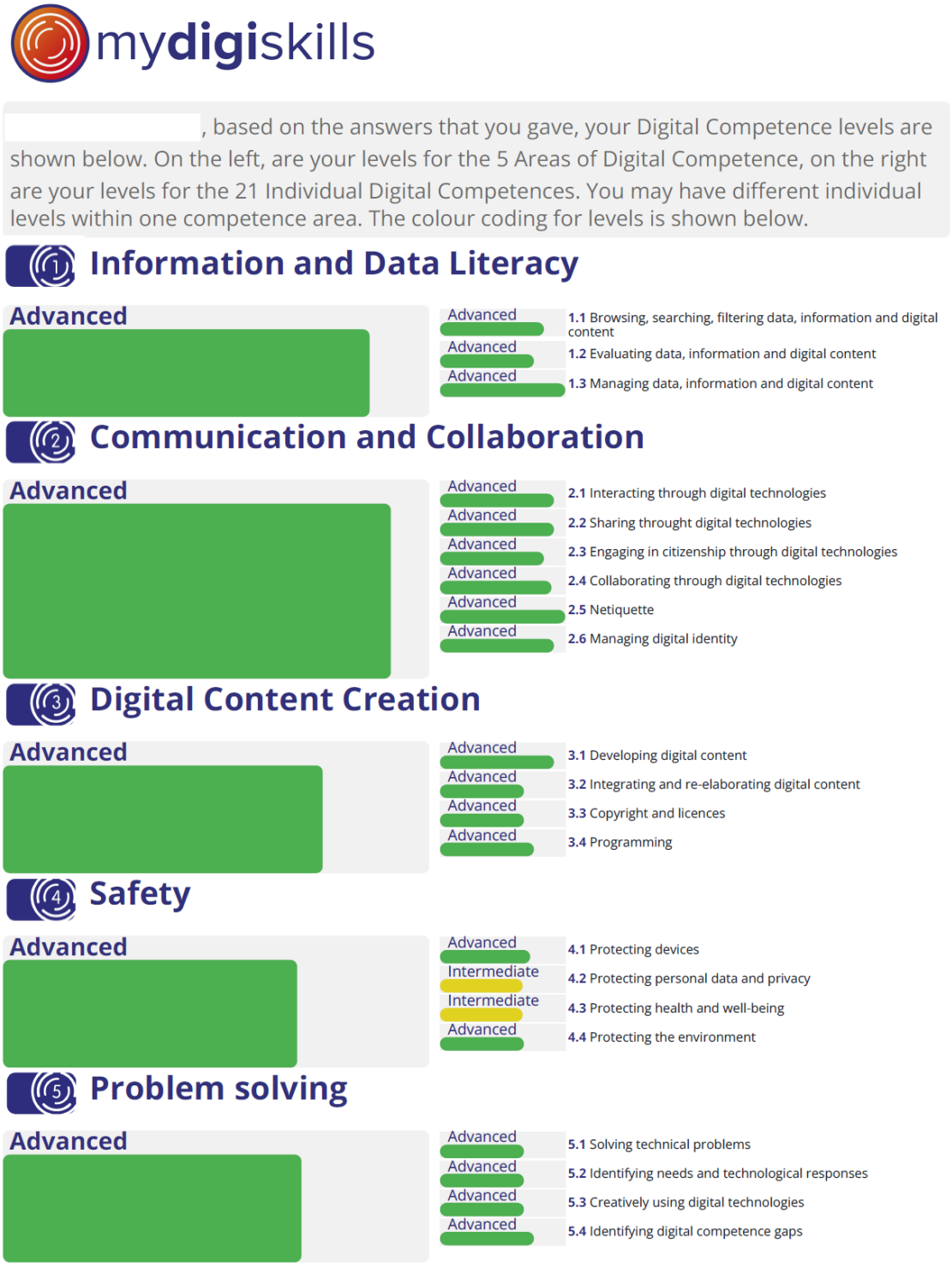

Figure 7. Example of MyDigiSkills self-assessment results based on the DigComp 2.1 Framework

As of March 2025, it has been announced that several schools in Tallinn will collaborate with the Estonian coding school [44]. Such collaboration is a good opportunity for schoolchildren to try programming. Events from large employers, career days, competi-

tions, and hackathons help people immerse themselves in the environment, improve their skills, and become part of a community of like-minded people.

Cybersecurity expert A (in Appendix 3) recommends developing “healthy paranoia” and developing critical thinking. He notes that cybersecurity is not only a lucrative career but also a socially significant one. Objective assessment of one’s skills and specialisation in a specific area, according to Expert B (Appendix 4), is important for professional growth. He also advises paying attention to details and reminds that cybersecurity professionals work to protect, not to harm. Expert C (Appendix 5) emphasises that technical skills and a deep understanding of the regulatory environment, as well as human psychology, are required in cybersecurity.

It is necessary to analyse, reflect, and ask yourself, "How can the material I am studying be applied?" AI is firmly entering our lives, and we should remember the security of our data. Discussing with close ones and helping the older generation observe safe cyberspace practices helps consolidate knowledge in practice and maintain the cyber resilience of the surrounding society. According to the World Economic Forum Report 2025, "79% of Estonian employers report skills gaps in the labour market, which they plan to address through reskilling and upskilling" [12]. Lifelong learning is already the norm, so learning the necessary skills "on the go" is becoming more accessible. Massive open online courses (MOOCs) taught by companies such as Google, IBM, Microsoft, influential universities, and other organisations provide in-demand and relevant knowledge (for example, platforms such as Coursera, Codecademy, Udemy, EdX). Some cybersecurity certificates can be obtained already in high school [45]. Developing attentiveness, critical thinking, technical skills, and information hygiene not only helps in further studies and careers but also contributes to safer behaviour in conditions of information overload.

4.3.3 Limitations of the Study and Recommendations for Future Research

The research was conducted at a private school where Estonian is the language of instruction. Despite its private ownership, the school is part of the state education system and complies with national educational standards.

- This community school has a unique learning environment and culture, which means that the results may differ significantly from those obtained in other schools across Estonia.
- Secondly, the number of participants was quite small – just 38 students in the

phishing simulation and only 3 respondents in the IT class student survey.
- In addition, the study avoided collecting any personal data in order to ensure anonymity. Because of this, it was not possible to study individual behaviour in more depth or compare results based on things like students' background knowledge or interest in the topic.
- Time constraints prevented us from assessing the effect of the course over time, before and after the cybersecurity course.
- Another problem is that the student survey was modified to have a smaller number of questions and fewer respondents.
- Of course, the research methods used only provide a fragmentary picture.

Looking ahead, there are several directions that could be explored in future research:

- Scaling up across schools with different resources. It would be useful to replicate a similar study in other schools – public and private, urban and rural – to see similarities and differences.
- Following students over time (a long-term study) could show whether and how cybersecurity education affects students' digital habits or career choices. This could include comparing an IT class before and after cybersecurity education. Then, comparing it to a control group, a non-IT class that did not have the subject.
- Focusing on teachers to assess the necessary methodological support could be an option for future research.
- Future research methods could include knowledge tests or behavioural experiments related to cybersecurity.
- As Estonia implements the AI Leap 2025 initiative, future research could examine how AI tools support students' understanding, engagement, and critical thinking when learning cybersecurity.

4.4 Conclusion

The research investigated the possibilities of building cybersecurity competence in high school students using a multidimensional framework including technical, pedagogical, cultural, ethical and social-engineering aspects. The empirical part was related to a public school in Estonia and included several methods: interviews with experts, phishing simulation, student survey and classroom observation.

The cultural analysis showed that Estonia's digitally developed society strongly influences students' perceptions and attitudes towards cybersecurity, answering SQ1.1 and SQ1.2. Students recognise its importance in everyday life, but show varying degrees of involvement

and responsibility.

Regarding SQ2.1, the technical component of the study showed that tasks such as password strength analyses and Python exercises, particularly those involving cyphers and simulations, were successful in promoting competence development (see Appendix 6). These activities also contributed to the development of SQ2.2 as they were embedded in the project-based and flipped classroom methodology. Combining technical learning with broader educational objectives such as communication, reflection and critical thinking. Instructor feedback confirmed that the combination of technical tasks with individual creativity and public speaking increased student motivation.

The results of the simulated phishing campaigns showed clear differences in awareness and response between IT and non-IT students, answering SQ3.1 and confirming that structured cyber security training increases resilience to social engineering. Regarding SQ4.1, several pedagogical barriers were noted during the interviews, including time constraints, technical challenges, and varying degrees of student preparedness. However, the flipped classroom and PBL methods were shown to increase engagement and autonomy, which supports SQ4.2 and confirms the literature evidence of their motivational value [20].

From an ethical perspective (SQ5.1), concerns about teaching potentially dangerous concepts (e.g. phishing or hacking) in the school context are poorly observed. Interviews identified the need to emphasise ethical frameworks to avoid inadvertently encouraging harmful behaviour. Experts pointed out that moral values are typically formed earlier upper secondary school and shaped individually. However, SQ5.2 related to that schools still play an important role: they can offer a structured and safe environment for teaching responsible cybersecurity, especially when ethical guidance and discussions are integrated alongside hands-on practice.

Overall, the findings suggest that cybersecurity skills can be effectively developed in secondary education through a blended approach—one that combines technical training with reflective, ethical, and socially relevant learning. The multidimensional framework used in this study helped capture both the tangible outcomes and the human aspects of cybersecurity education within a real school setting.

5. Summary

This study investigates the current state of cybersecurity education in Estonian secondary schools using a private Estonian-language upper secondary school as an example. The study combined several empirical methods: interviews with experts, student surveys, classroom observation and a phishing simulation involving 12th grade students.

Clear differences in digital awareness and behaviour were found between students in IT-focused programmes and those in other areas (Figure 3). These results support the idea that specialised cybersecurity education improves students' understanding of digital risks.

Among the challenges hindering the adoption of cybersecurity education, experts identify a lack of qualified teachers, a lack of a national curriculum, and a decline in the attractiveness of the teaching profession. There are also some concerns about how to responsibly teach potentially sensitive content. Education experts emphasised the benefits of project-based and interdisciplinary learning to keep students interested. At the same time, industry representatives called for a greater focus on stewardship, early ethical education and closer co-operation with the private sector.

In conclusion, the study emphasises that building a sustainable digital society depends on a systemic, interdisciplinary and value-based approach to education. Ethics and critical thinking should accompany the teaching of technical skills, starting from school.

References

[1] Ministry of Economic Affairs and Communications of Estonia. *Cybersecurity Strategy 2024–2030: Cyber-Conscious Estonia*. Tech. rep. Accessed: May 12, 2025. Government of Estonia, Mar. 2024. URL: https://www.mkm.ee/sites/default/files/documents/2024-12/Cybersecurity%20strategy%202024%E2%80%932030%20Cyber-conscious%20Estonia.pdf.

[2] European Commission / EACEA / Eurydice. *Informatics Education at School in Europe: Eurydice Report*. Tech. rep. Publications Office of the European Union, 2022. DOI: 10.2797/393964. URL: https://eurydice.eacea.ec.europa.eu/publications/informatics-education-school-europe.

[3] Kirsti Melesk et al. *Labour Force and Skills Needs in Cyber Security in Estonia: Main Conclusions*. Tech. rep. Accessed: May 12, 2025. PRAXIS Centre for Policy Studies, Mar. 2019. URL: https://www.praxis.ee/uploads/2018/04/K%C3%BCberturbe-uuring.-L%C3%BChikokkuv%C3%B5te_eng.pdf.

[4] Birgy Lorenz et al. "Cybersecurity Within the Curricula of Informatics: The Estonian Perspective". In: *Informatics in Schools: Situation, Evolution, and Perspectives. ISSEP 2019. 12th International Conference*. Vol. 11984. Lecture Notes in Computer Science. Springer, Nov. 2019, pp. 159–180. DOI: 10.1007/978-3-030-33759-9_13. URL: https://link.springer.com/chapter/10.1007/978-3-030-33759-9_13.

[5] Harno (Education and Youth Board of Estonia). *e-Koolikott*. Accessed: May 12, 2025. 2025. URL: https://e-koolikott.ee.

[6] Safer Internet Centre in Estonia. *Targalt Internetis – Safe Internet Use*. Accessed: May 12, 2025. 2025. URL: https://www.targaltinternetis.ee.

[7] Harno (Education and Youth Board of Estonia). *ProgeTiigri kogumik: Digital Learning Resources for Technology and Programming Education*. Accessed: 2025-05-02. 2025. URL: https://progetiiger.ee/.

[8] United Nations Department of Economic and Social Affairs (UN DESA). *E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development*. Tech. rep. Accessed: May 12, 2025. United Nations, Sept. 2024. URL: https://publicadministration.un.org/en/.

[9] Piret Pernik. “Cybersecurity Education in Estonia: Building Competences for Internal Security Personnel”. In: *Proceedings of the Estonian Academy of Security Sciences* 18 (2019), pp. 71–108. DOI: 10.15158/gtsn-7h55. URL: https://digiriiul.sisekaitse.ee/handle/123456789/3122?locale-attribute=en.

[10] Tommaso De Zan and Fabio Di Franco. *Cybersecurity Skills Development in the EU*. Tech. rep. European Union Agency for Cybersecurity (ENISA), Dec. 2019. DOI: 10.2824/525144. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20Skills%20Development%20in%20the%20EU.pdf.

[11] Eric Hazan et al. *The Race to Deploy Generative AI and Raise Skills*. Accessed: May 12, 2025. May 2024. URL: https://www.mckinsey.com/mgi/our-research/a-new-future-of-work-the-race-to-deploy-ai-and-raise-skills-in-europe-and-beyond.

[12] World Economic Forum. *The Future of Jobs Report 2025*. Tech. rep. Accessed: May 12, 2025. World Economic Forum, Jan. 2025. URL: https://www.weforum.org/publications/the-future-of-jobs-report-2025/.

[13] European Union Agency for Cybersecurity (ENISA). *Cybersecurity Education Initiatives in the EU Member States*. Tech. rep. ENISA, Dec. 2022. DOI: 10.2824/486119. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA_Cybersecurity%20education%20initiatives%20in%20MS.pdf.

[14] Riina Vuorikari, Stefania Kluzer, and Yves Punie. *DigComp 2.2: The Digital Competence Framework for Citizens – with new examples of knowledge, skills and attitudes*. Publications Office of the European Union. Accessed: May 12, 2025. 2022. URL: https://op.europa.eu/en/publication-detail/-/publication/50c53c01-abeb-11ec-83e1-01aa75ed71a1/language-en.

[15] CybExer Technologies. *Cyber Battle of Estonia*. Accessed: May 12, 2025. 2024. URL: https://cybexer.com/case-studies/cyber-battle-of-estonia/.

[16] Estonian Ministry of Defence. *About the Project – CyberOlympics Estonia (Küber-Naaskel)*. Accessed: May 12, 2025. 2025. URL: https://sites.google.com/view/kyberolympia/eng/about-the-project.

[17] CTF Tech. *Telia CBoNB'24 & CyberSpike - Cybercation*. https://ctftech.com/teliacbonb24-cyberspike-cybercation/. Accessed: May 12, 2025. 2024.

[18] Birgy Lorenz and Kaido Kikkas. "'Trust Me, You Will Need It': Cybersecurity as Extracurricular Subject at Estonian Schools". In: *Educational Technology in Practice: Research and Practical Case Studies from the Field*. Ed. by Don Passey et al. Springer, 2020, pp. 175–188. ISBN: 978-3-030-50308-6. DOI: 10.1007/978-3-030-50309-3_12.

[19] Ying Wang and Yuxuan Qian. "Flipped Classrooms in K–12 Education: A Meta-Analysis of Effects on Academic Achievement". In: *Review of Educational Research* 94.1 (2024), pp. 89–125. DOI: 10.3102/00346543241261732. URL: https://journals.sagepub.com/doi/10.3102/00346543241261732.

[20] Lu Zhang and Yan Ma. "A study of the impact of project-based learning on student learning effects: a meta-analysis study". In: *Frontiers in Psychology* 14 (2023), p. 1202728. DOI: 10.3389/fpsyg.2023.1202728. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2023.1202728/full.

[21] Thinkst Applied Research. *Canarytokens: Free, Quick, Detection for Intrusions*. Accessed: May 12, 2025. 2025. URL: https://canarytokens.org/.

[22] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. "Phishing in Organizations: Findings from a Large-Scale and Long-Term Study". In: *2022 IEEE Symposium on Security and Privacy (SP)*. 2022, pp. 842–859. DOI: 10.1109/SP46214.2022.9833766.

[23] Rainer Kattel and Ines Mergel. "Estonia's Digital Transformation: Mission Mystique and the Hiding Hand". In: *Great Policy Successes*. Ed. by Paul 't Hart and Mallory Compton. Accessed: May 12, 2025. Oxford: Oxford University Press, 2019. DOI: 10.1093/oso/9780198843719.003.0008. URL: https://doi.org/10.1093/oso/9780198843719.003.0008.

[24] The Education and Youth Board. *Tiiger – Hariduse tehnoloogiakompass*. Accessed: May 12, 2025. URL: https://kompass.harno.ee/tiigrihupe/algus/.

[25] Kristiina Kriisa. *Estonia: 100% Digital Government Services*. Accessed: May 12, 2025. Jan. 2025. URL: https://e-estonia.com/estonia-100-digital-government-services/.

[26] Estonian Business and Innovation Agency. *The Full List of Estonian Unicorns*. Accessed: May 12, 2025. 2023. URL: https://investinestonia.com/the-full-list-of-estonian-unicorns/.

[27] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024*. Tech. rep. ENISA, Sept. 2024. DOI: 10.2824/0710888. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf.

[28] Presidential Digital Council of Estonia and Ministry of Education and Research of Estonia. *TI-Hüpe: Official Page of AI Leap 2025 Educational Programme*. Accessed: May 12, 2025. 2025. URL: https://aileap.ee/en.

[29] Estonian Ministry of Education and Research. *Estonia Announces A Groundbreaking National Initiative: AI Leap Programme to Bring AI Tools to All Schools*. Accessed: May 12, 2025. Feb. 2025. URL: https://www.hm.ee/en/news/estonia-announces-groundbreaking-national-initiative-ai-leap-programme-bring-ai-tools-all.

[30] Niklas Humble. "A conceptual model of what programming affords secondary school courses in mathematics and technology". In: *Education and Information Technologies* 28 (8 Aug. 2023). Accessed: May 12, 2025, pp. 10183–10208. ISSN: 15737608. DOI: 10.1007/S10639-023-11577-Z/FIGURES/1. URL: https://link.springer.com/article/10.1007/s10639-023-11577-z.

[31] U.S. Cybersecurity and Infrastructure Security Agency (CISA). *Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats*. Tech. rep. Accessed: May 12, 2025. U.S. Department of Homeland Security, Jan. 2023. URL: https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c_0.pdf.

[32] Information System Authority (RIA). *Estonian Schools Should Prioritise Cybersecurity*. Accessed: May 12, 2025. 2024. URL: https://www.ria.ee/en/estonian-schools-should-prioritise-cybersecurity.

[33] MITRE ATT&CK. *Enterprise ATT&CK Matrix – Version 16.1*. Accessed: May 12, 2025. Dec. 2023. URL: https://attack.mitre.org/versions/v16/matrices/enterprise/.

[34] Information System Authority (RIA). *Cyber Security in Estonia 2025*. Tech. rep. Accessed: May 12, 2025. Information System Authority (RIA), Feb. 2025. URL: https://www.ria.ee/sites/default/files/documents/2025-02/Cyber-security-in-Estonia-2025.pdf.

[35] Organisation for Economic Co-operation and Development. *PISA 2022 Results (Volume I): The State of Learning and Equity in Education*. Tech. rep. OECD Publishing, 2023. DOI: 10.1787/53f23881-en. URL: https://www.oecd.

org/publications/pisa-2022-results-volume-i-53f23881-en.htm.

[36] Organisation for Economic Co-operation and Development. *PISA 2018 Results (Volume I): What Students Know and Can Do*. Tech. rep. OECD Publishing, 2019. DOI: 10.1787/5f07c754-en. URL: https://www.oecd.org/publications/pisa-2018-results-volume-i-5f07c754-en.htm.

[37] Republic of Estonia, Government. *Gümnaasiumi riiklik õppekava [National Curriculum for Upper Secondary Schools]*. Accessed: May 12, 2025. Mar. 2023. URL: https://www.riigiteataja.ee/akt/108032023006.

[38] Enefit Green. *Enefit Green partners with Sumitomo Corporation to develop Liivi Bay offshore wind farm*. Accessed: May 12, 2025. Feb. 2025. URL: https://enefitgreen.ee/en/-/uudised/enefit-green-ja-sumitomo-corporation-alustavad-koostood-liivi-lahe-meretuulepargi-arendamiseks.

[39] RB Rail AS. *Rail Baltica continues work on the implementation of a Public-Private Partnership model to lessen the burden on state budgets during construction*. Accessed: May 12, 2025. Aug. 2024. URL: https://www.railbaltica.org/rail-baltica-continues-work-on-the-implementation-of-a-public-private-partnership-model-to-lessen-the-burden-on-state-budgets-during-construction/.

[40] eKool AS. *eKool: the Ultimate Educational Platform*. Accessed: May 12, 2025. 2025. URL: https://www.ekool.eu/en/home.

[41] Eve Mägi et al. *Enhancing Public-Private Partnership and the Role of EdTech in Advancing Inclusive Education in the Baltics*. Policy Brief. Co-funded by the European Union. Praxis Centre for Policy Studies, 2021. URL: https://www.praxis.ee/uploads/2015/08/BRT_Public-private-partnership.pdf.

[42] Information System Authority (RIA). *Cyber Test*. Accessed: May 12, 2025. 2025. URL: https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/kubertest.

[43] ALL DIGITAL AISBL. *MyDigiSkills Test*. Accessed: May 12, 2025. 2025. URL: https://mydigiskills.eu/test/index.

[44] Invest in Estonia. *Estonian High Schools to Launch kood/Jõhvi Programming Courses*. Accessed: May 12, 2025. Mar. 2025. URL: https://investinestonia.com/estonian-high-schools-to-launch-kood-johvi-programming-courses/.

[45] CYBER.ORG. *Empowering Educators to Teach Cyber*. Accessed: May 12, 2025. 2025. URL: https://cyber.org/.

[46] Information System Authority (RIA). *RIA CyberMeetup*. Accessed: May 12, 2025. Estonian Information System Authority. 2025. URL: https://www.ria.ee/en/cyber-security/national-coordination-center-ncc-ee/ria-cybermeetup.

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis[1]

I, Anastasiia Shapran,

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Empowering high school students in cybersecurity: a multi-dimensional approach (the case of one Estonian school)", supervised by Olaf Manuel Maennel and Oleg Shvaikovsky.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

12.05.2025

[1]The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Interview Questions for Cybersecurity Experts

The following questions were asked during two semi-structured interviews (Expert A and Expert B) and one email-based written interview (Expert C) with cybersecurity experts as part of the thesis research.

1. How do you assess young people's (e.g., high school graduates or interns) attitudes towards cybersecurity? How aware are they of the digital risks? Please, tell me about your "pain" as an employer (e.g. staff shortage).
2. What skills or behavioural models do you consider critical for protection against social engineering?
3. Does your organisation have any internal practices (training, simulation, onboarding) to prevent social engineering attacks, and how effective are they?
4. What knowledge gaps do you most frequently observe among young specialists? Are they technical skills, programming knowledge, digital ethics, soft skills, or something else? Does their IT preparation at school (e.g., IT-direction class in gymnasium, participation in hackathons, Olympiads) affect this?
5. Do you see the possibility for closer public-private cooperation in developing digitally competent professionals? Could you imagine yourself teaching at school someday (e.g., teaching an elective course for high school students or conducting a practical session as part of a course)?
6. Which educational methods or formats (e.g., hands-on training, case studies, attack simulations) are most effective in teaching cybersecurity? Please share your suggestions.
7. How important is it to teach ethical aspects to future professionals (e.g., the use of AI at work and behaviour in the digital world in general)?
8. Where do you think the line lies between teaching technical skills (ethical hacking, vulnerability analysis) and the risk of promoting dangerous behaviour in cybersecurity field (to grow a bad hacker)?
9. What values should be offered to future cybersecurity professionals during the schooling phase?
10. What recommendations would you give to the school community (curriculum developers, principals, teachers) to help them better prepare students for the digital world and a career in IT and cybersecurity?

Appendix 3 – Interview Transcript: Cybersecurity Expert A

Interviewee (Expert A): JÜRGEN ERM, 15 years in IT, including 8 years in Cybersecurity
Position: CEO, NEVERHACK Estonia (previously CYBERS)
Interviewer: Anastasiia Shapran
Date: 26 April 2025
Duration: 35 minutes
Language: English (translated from Estonian)

Interviewer (I.) Thank you for agreeing to be interviewed. We will try to follow the pre-formulated questions with some clarifying questions on my part. How do you assess young people's (e.g., high school graduates or interns) attitudes towards cybersecurity? How aware are they of the digital risks?

Expert (E.) I can't say about high school leavers, but the youngest employees come to us from around the second year of university at the earliest, I'd say from around the second year. The level of expectations in the field is such that a university doesn't prepare you fully for real-world work, not even internships. So, it's hard for me to assess that point objectively. I haven't reviewed it thoroughly.

I. But do you generally experience a "pain point"? For example, not having enough specialists?

E. Yeah, that's something we all experience. It's not just us. There's a significant shortage of cybersecurity specialists in Estonia. We're constantly competing for the same good experts. Our company has even had to hire people from abroad because there are just not enough specialists here.

I. In your opinion, are young people today aware of digital threats?

E. It's my opinion, but I think some students are very aware—some, not at all. Considering how much this topic is talked about in the media and in schools, I hope the awareness and understanding of the need for cybersecurity is growing. But again, I can't give solid numbers—just a gut feeling.

I. Thank you. Second question—what skills or behavioural models are critical for defending against social engineering?

E. These skills all start with awareness. If someone knows what threats they might face, they're more likely to recognise them in the moment. And as for behavioural models, I'd say a kind of "healthy paranoia" is necessary. Especially online and in digital communication, you must always keep your guard up. Phishing and manipulation attempts are often very clever, and they prey on human weaknesses by creating fear or urgency, for example. You have to recognise those moments and stop yourself, take a step back and let your rational mind assess the situation.

I. Do you see opportunities for closer collaboration between the private sector and education in developing skilled professionals?

E. Yes, absolutely. We already cooperate extensively with the public sector—for example, with RIA and CERT Estonia. We run awareness campaigns and help resolve incidents with clients. This cooperation works very well. Both my colleagues and I have visited schools to give occasional guest lectures or share real-world examples. It's something we've done and will definitely continue doing.

I. Would you personally consider teaching in a school?

E. I don't know if I'd want to be a full-time teacher, but I'd be happy to share my experience. When I was in school, it was always eye-opening when professionals came to talk about what real work looks like. I think every company should take responsibility for the next generation that way.

I. Thank you. What teaching methods or formats do you think are most effective for cybersecurity?

E. Well, effectiveness comes from a complete package. First, students need a base of theoretical knowledge to build on. Then, the fastest development happens through practice. Looking at our colleagues who come straight from school, we see the quickest growth when we get them directly involved in real work, when they're working alongside experienced specialists and can ask questions and get hands-on experience. That's what I think is most important in cybersecurity. The practical side really matters, and it should be integrated as much as possible into school programs.

I. Do you think phishing simulations are a good format?

E. Honestly, phishing simulations are overrated. There are several strong studies showing their actual effectiveness is very low. They don't really change people's behaviour. Awareness improvements from them barely appear in the statistics, often in the single-digit percentages. So, the impact is quite minimal.

I. Why do you think that is?

E. The problem is that the simulation hits people randomly during their workday. They're not mentally engaged when it happens. Even if they click the link, they don't "switch on" and say, "Okay, I'm learning something now, so I don't repeat this mistake."' They just click through and move on with their day. Work needs to get done. So, it doesn't capture their attention in a way that triggers real behavioural change. If you're interested, I can send you a link with the research and resources—it paints a clear picture. Giving people the time and space to think actually helps. You need deeper, more thorough training with a strong practical component. It's not enough to just say, "Don't click suspicious links." You have to show them what really happens when you do. Show them how easy it is to craft a phishing email or attach a virus to an Excel file. These tools are easily available today. I think seeing that reality hits home much better.

I. How important is it to teach ethics to future cybersecurity professionals?

E. Very important. I once visited a high school and met a few students who were already quite skilled—they could carry out fairly sophisticated attacks. I had to explain to them that what they were doing was illegal, even if they were experimenting. Many young people are naturally curious and want to push boundaries, which is fine, but without understanding the legal and ethical limits, they could ruin their future careers with one bad decision.

I. So, do technical skills and ethics need to be taught together?

E. Yes, absolutely. From my university experience, I remember that ethical aspects were clearly part of the curriculum. We covered them multiple times. I'm not sure how it's done in high school, though. I went to a school with an economics focus, so I don't recall anything like that being discussed — but that was quite a long time ago.

I. Where do you think the line lies between teaching technical skills and encouraging risky behaviour?

E. I think those two things — technical knowledge and behaviour —shouldn'tt be bundled together as if one leads to the other. We must teach technical skills as well as we possibly

can. What an individual does with that knowledge afterwards — whether they stay in the professional field or enter the criminal world — is up to their moral compass. It would be wrong to think, “Let’s teach them less just in case they turn bad.” That’s not the right approach. We must train our specialists to the best of our ability and trust that 99% of people are good. Of course, there will always be that 1% or 2% who choose a criminal path —that’s always been part of human nature, even before the internet.

I. What values should we promote while educating future cybersecurity specialists?

E. We should keep promoting cybersecurity as a rapidly developing and very lucrative career. Cybersecurity specialists are well-paid. Even if you’re fresh out of school, you can earn a decent salary immediately. I remember one case — I hired a young guy, and later, he told me,“You know, my parents are both teachers, and now I make more than they do.” He said,“When I told them my salary, they were like — wow, we’ve worked for 20 years, and now you’re earning more straight out of school.” That was a striking moment. But with all those benefits, we also have to emphasise social responsibility—that’s key. This field isn’t just about money—people working in cybersecurity are protecting our society, helping to block threats, and keeping our digital country running, that is a valuable and important value in itself.

I. So, young people need to know that a cybersecurity career is accessible?

E. Yes, absolutely. It’s very accessible. If someone goes to TalTech after high school to study cybersecurity, they can start working immediately after graduation. I honestly don’t know any cybersecurity specialists who are unemployed right now. This field is growing rapidly, and you can work in Estonia or abroad. Of course, it’s important to feel that this is the right field for you. I’vee also seen cases where someone starts studying cybersecurity thinkingit’ss their thing, but after a while, they realizeit’ss not. That’s true of any field — in the end, people must find what they want to do. You can’t just force yourself into something that doesn’t fit.

I. I’ve heard that there are cases where people start working in cybersecurity right after finishing school?

E. But yes, they do start working right away. Well...I’d say when we hire someone straight out of school, they usually become fully productive within six months. For some, it takes one month, for others, six months, but within six months at the latest, we have specialists ready to be used for specific work tasks.

I. Do you have the resources to train and mentor these young people? Or is it easier when a candidate already has experience?

E. Well, the thing is, we have different positions—some require years of experience. But we also have roles where we can train people ourselves. So, these two approaches don't conflict; they coexist. Now, regarding question 10, what could be offered to the school community? One very cool initiative currently underway is the increasing integration of artificial intelligence into the entire school system. This AI leap, which is now reaching schools, will be a critical driver of success for both educational institutions and society in the next 10 years. I strongly encourage participating in this as much as possible because it supports cybersecurity awareness. And for schools, especially high schools, I think a great recommendation would be for them to confidently approach any Estonian cybersecurity company. They can invite professionals, for example, to give occasional lectures or lessons—people who can explain how things work in practice.

I. How would you comment on the fact that informatics is currently not mandatory in the school curriculum?

E. Well, I'm not exactly up to date, but if it's not yet included in the national curriculum of schools, then I think we definitely need to change that—because Estonia is an IT country. And if students are already introduced to this field during high school, then maybe we'll have more applicants for cybersecurity-related programs at universities. I see that as a good springboard.

I. That was great. Thank you for the interview!

E. Thanks, and good luck with your work!

End of Interview

Appendix 4 – Interview Transcript: Cybersecurity Expert B

Interviewee (Expert B): MYKHAILO MAHUN, 22 years in IT, including 18 years in Cybersecurity
Position: CEO, ALLCONTROLS OÜ, Estonia
Interviewer: Anastasiia Shapran
Date: 25 April 2025
Duration: 40 minutes
Language: English (translated from Russian)

Interviewer (I.) Thank you for taking the time to speak with me. You are a manager and a practising auditor with extensive experience and international exposure. How would you assess young people's — for example, high school students or interns — attitudes toward cybersecurity? How aware are they of the risks in the digital environment? What issues do you see as an employer?

Expert (E.) Are we talking specifically about young people who are technically oriented and aiming for careers in the IT and cybersecurity industry? Or are we speaking more generally?

I. Generally, it is whoever you've had the chance to meet.

E. There are different types, such as cybersecurity enthusiasts, who understand current trends, attacks, and how to protect assets. Then, some haven't yet chosen a specialisation, with a surface knowledge but high confidence and pose a particular risk. An employer must understand that someone might lack real competence but still be convinced they "know everything" because they're "good with computers". That's why onboarding is essential: explain what corporate information is, how we protect it, what's allowed and what isn't — just like with any other employee. For example, we don't get interns straight out of school. They come to us at least in their final year of university. As a rule, they are technically literate specialists whom I interviewed; they already have a more or less good understanding of the digital environment.

I. Overestimating skills can be dangerous for the person themselves — they might fall into a trap, right?

E. It's not only in cyber security; I would say it's in any field; it's probably a dangerous misconception. Sometimes, there are places where good competencies are needed and expected. A person with very superficial knowledge can do harm because of such a sloppy attitude and a lack of understanding of processes and rules. But here, from the point of view of how an organisation can protect its information. If we talk about risk in general, we can probably say the same. Suppose a trainee has an infected computer, which he will plug in somewhere. He can use it to process some tasks given to them or work with some company data. It's all about how it's organised.

I. Let's move smoothly to question 2. What skills or behaviours are critical to protecting against social engineering attacks?

E. Well, there are quite a lot of materials on this topic. Modelling such attacks in the corporate segment is essential, on their own or with third parties' help. It is good to organise testing and simulation of phishing attacks to check the general picture and conclude. Let's say that people were deceived by phishing. We need to determine the percentage of those affected and conduct training for all employees and separate training for those who fell victim to the attack. This process should be repetitive. Large companies often conduct continuous phishing simulations across different departments with various scenarios to keep employees aware and prepared. It's also essential to prepare the right content for onboarding. Employees usually don't like to read some boring policies. You can prescribe a cool policy that is big and beautiful, but it will not be readable. A team of cybersecurity experts will be involved. Still, most of us may find it hard to understand and will likely forget the details soon. Training should feature interactive content and concise presentations or brochures. As red flags, it can be an urgent call to action or intimidation. Employees should report concerns to the information security team. Training should involve simulations of phishing attempts, guided by someone knowledgeable on current trends, as the average user may struggle to identify these threats. Employees should also exercise caution when clicking links, especially those sent to personal accounts.

I. What do you think of my idea of a phishing simulation that I talked about before the interview?

E. The fact that someone clicks is already a signal. But just clicking isn't enough — knowing who enters credentials is essential. That's a higher level of analysis. Also, you can't rely solely on email provider protections. Settings must be customised, SPF (Sender Policy Framework) are necessary. That's a job for technical specialists. We can't put all the responsibility on users. A comprehensive approach is essential: training plus technical measures. There are companies where 25% of users enter their credentials on fake sites

and others where it's just 1% — and that's a big difference.

I. Which of these practices do you use in your company?

E. We use training and technical configurations — as part of our standard package. We're a small company, so everything's visible, and we haven't had issues so far. We try to keep even non-tech staff informed.

I. What knowledge gaps do you observe in junior specialists?

E. The usual ones are how to work with corporate services and where to store documents (not locally, but in the cloud, and not personal cloud, but corporate). Communication inside and outside the company, as well as how to format emails — all of that needs to be taught. It's normal — if someone hasn't encountered it before, they won't know. That's why clear explanations and basic information security requirements are essential.

I. Have you ever noticed that the cool specialists working today have backgrounds that include participating in various hackathons since school? Is there a specific time that is better to start?

E. I would say that I don't see such a direct dependence in my practice. Some guys studied more than that. There, for example, in a technical university, and then re-qualified; in principle, they became quite good technicians, administrators, and so on. But again, it is hard for me to estimate those who are graduating from university now, and I have a small sample here. For example, I am talking about those generations who graduated 5-6 years ago. I am sure the situation may be different now, so I would try to collect more up-to-date information from other interviewees. Maybe there are those who have such an academic background, and they like to be recognised there. But maybe they want to teach themselves. Well, I think such people don't always want to work in commercial organisations, and often they can stay teaching or working somewhere. Perhaps it could be interesting or even more interesting in companies that focus on teaching or in certain state projects.

I. Do you think programming skills are necessary for cybersecurity professionals?

E. Basic knowledge of at least one language is a must. However, there are many roles in cybersecurity, such as compliance, standards implementation, and administration. Some of these may not require in-depth programming skills, but the technical basics are still necessary. You should at least understand how scripts, databases, and networks work.

University level basics are essential. Cryptography is, too.

I. The 12th graders at the school I'm writing about took a Python course that included cryptography tasks.

E. That's great. You can't properly analyse vulnerabilities without understanding the code. You don't have to be an expert, but the basics are necessary.

I. Do you see potential for public-private partnerships in training? Are you considering teaching opportunities?

E. In theory, yes. In practice it is difficult due to time constraints. Online, it is possible. However, the topic should be relevant for schools. Co-operation between universities and business already exists. For example, I got my first job while writing my bachelor's thesis thanks to the co-operation between university and company. Private companies are definitely interested in talent, and internships help to identify good candidates and reduce hiring risks.

I. Only large companies can afford to train interns because they have the resources.

E. For the most part, yes. However, even small companies have routine tasks that can be combined with training. For example, working in the helpdesk is not too difficult, but useful. You learn by doing and can gradually grow.

I. If you were to take on an employee now, knowing that he is fully technically savvy but just a theorist who has just come out of the university, what approach would be appropriate and educational for him?

E. Well, if we are talking about information security auditor, then perhaps this assistance can be in the preparation of a report, their presence at the interview, and the performance of some routine work, which is clear enough and relatively simple. Understand what it is in general and how it is compiled. Of course, you should start with the fact that he had just generally familiarised himself with some kind of, let's say, the standard, which is carried out audit.

I. How important do you think it is to train young professionals in ethical aspects, such as using artificial intelligence and behaviour in the digital world?

E. This is quite important. Everything is now regulated: there are clear legal consequences

for certain actions, and not necessarily malicious - even negligence can break the law. Therefore, you need to understand the basics: what intellectual property is, how it is protected, and what responsibility there is for it. If we are discussing system testing or hacking practices, for example, it is necessary to request authorisation in advance. Otherwise, actions may be classified as unlawful, with appropriate consequences. **I.** Do you use artificial intelligence in your work?

E. Well, yes, of course, I think everyone already uses it, but we also have a policy. There are, let's say, requirements that when using the artificial intelligence system, you have to exclude sensitive data, personal data. The other thing is already how to further these results. They can adapt them to their task. In the same way, everyone probably uses it for self-study. It is quite an effective tool, but it requires double-checking, i.e. you cannot trust it blindly.

I. Even if you turn off the option to train the model, is it still risky to input sensitive data?

E. Yes. Even with a corporate subscription, it's better to avoid sensitive data. Usually, there's no need for it. If large datasets need to be processed, use your own models.

I. Where's the line between teaching and the risk of "raising a hacker"?

E. Clear explanation is needed: what's legal and not — and the consequences, especially for young people. Even a minor violation can ruin a career. It's the same in any field — temptation, but you must have personal responsibility. A cybersecurity professional should work to protect, not to harm.

I. What values should be taught?

E. The field is complex, and it is actively developing, so you need to be on the trend. Maybe you should choose one thing and specialise. Someone will be, let's say, a great network specialist, someone will understand how to check the source code, or it can be interrelated things, someone will be interested in compliance audits in consulting in general, someone will be just a project manager in the end, and you should be able to do that too, and there are pros and cons there. On the one hand, you need to understand the industry. On the other hand, it is probably advantageous to always choose an area where you will have a direct latch to look for knowledge. Again, to understand the goals in general, so that there is no security for the sake of security. That is life itself; some basics are generally based on risk assessment.

I. How can schools help students prepare for digital life and careers?

E. There is a basis for informatics and computer science in school. And for some of them, it depends very much on the teacher. Well, in general, I am sceptical that someone can take, teach, but he can push to learn. Yes, to explain some aspects, principles, and basic principles. To try, to study and improve your knowledge, and to have the opportunity to develop in this area and, again, not only in cyber security. That's probably how it works in school. At the same time, if someone is interested in this, it is necessary to create an environment where this would be possible with the help of some additional classes. Again, this seems to me very subjective and depends on the teacher and his motivation. How interested he'll be. In addition, there are courses that are parallel to the school. Additionally, they receive already specific knowledge, and after such, courses can certainly be good enough. Practically, some experience can be gained already. Is it worth going straight after school to work? That's not what I would like to say unequivocally, it's probably very individual. So, maybe he will want to do his first correspondence course and go straight to work, so why not?

I. In Estonia, informatics is not yet mandatory in the national curriculum, but it will be by 2030. In some high schools, there are IT profiles and electives.

E. If that's the case, conveying the basics of cyber hygiene is all the more important. We live in a digital world, and even if not everyone will go into IT — everyone should have foundational knowledge. That's the responsibility of both schools and parents.

I. Thank you very much for the conversation!

E. You're welcome. Feel free to reach out with more questions.

End of Interview

Appendix 5 – Interview Protocol: Cybersecurity Expert C

Interviewee (Expert C): HANNA, 24 years in IT, including 21 years in Cybersecurity
Position: Deputy CISO in a fintech company, Estonia.
Interviewer: Anastasiia Shapran
Date: 30 April 2025
Form: written, by e-mail
Language: English

Interviewer (I.) How do you assess young people's (e.g., high school graduates or interns) attitudes towards cybersecurity? How aware are they of the digital risks? Please, tell about your "pain" as an employer (e.g. staff shortage).

Expert (E.) I do not really work with young people that much. Staff shortage is a thing for sure, especially in the second and third lines of defense where you're supposed to demonstrate not a single isolated technical skill which may be enough for the first line on certain positions but rather a broader understanding of tech, governance, people and regulatory landscape.

I. What skills or behavioural models do you consider critical for protection against social engineering?

E. A certain level of resiliency under pressure. Quite some social engineering scenarios are built around time, situational or hierarchical pressure.

I. Does your organisation have any internal practices (training, simulation, onboarding) to prevent social engineering attacks, and how effective are they?

E. Yes, we do phishing simulation exercises and information security trainings. Judging by numbers and cases reported to SOC, it works to a certain extent but you're never 100% bulletproof when it comes to social engineering.

I. What knowledge gaps do you most frequently observe among young specialists? Are they technical skills, programming knowledge, digital ethics, soft skills, or something else? Does their IT preparation at school (e.g., IT-direction class in gymnasium, participation in hackathons, Olympiads) affect this?

E. Almost no experience with young specialists, again, but from the ones I have seen it seemed that governance aspects often get underestimated in education in favour of pure technology.

I. Do you see the possibility for closer public-private cooperation in developing digitally competent professionals? Could you imagine yourself teaching at school someday (e.g., teaching an elective course for high school students or conducting a practical session as part of a course)?

E. Sure, we had initiatives like that organised and supported by my previous employers.

I. Which educational methods or formats (e.g., hands-on training, case studies, attack simulations) are most effective in teaching cybersecurity? Please share your suggestions.

E. The combined ones built on a good understanding of people's psychology, first of all. Not too tech, not too fluffy, but finding the right compromise for each audience is an art by itself.

I. How important is it to teach ethical aspects to future professionals (e.g., the use of AI at work and behaviour in the digital world in general)?

E. There should be something very basic but speaking AI, I'm not entirely sure we have a well-developed ethics for that as a species. So in that case Id rather emphasise the importance of open discussions.

I. Where do you think the line lies between teaching technical skills (ethical hacking, vulnerability analysis) and the risk of promoting dangerous behaviour in cybersecurity field (to grow a bad hacker)?

E. We're teaching how to cut people open in med schools and how to manipulate the regulations in law schools and then let people decide how to apply the knowledge within the existing legal framework of the state. I do not see much difference here TBH. If you know how to fix a water pipe, you know how to break a water pipe. It's always been and will be the case in any field.

I. What values should be offered to future cybersecurity professionals during the schooling phase?

E. I'm not sure you can manipulate the person's values that much at that stage; it normally

happens way before they reach the high school age.

I. What recommendations would you give to the school community (curriculum developers, principals, teachers) to help them better prepare students for the digital world and a career in IT and cybersecurity?

E. Please consider the governance aspects of cybersecurity and please emphasise the importance of solid foundation built on upper management commitment. We get so many not-so-young specialists who honestly believe that the whole cybersecurity thing is about firewalls and antiviruses while primarily it is about people and rather complex structures built of people, technical solutions, processes, policies and regulations.
Also, asset and configuration management: never sexy, always boring and always underestimated as a not purely cybersec thing while being the only real foundation for any cybersec.
Also, business context. We have so many security tools these days which produce thousands of records and findings and even offer some proprietary post-processing for them to limit the critical scope. And all of that is very nice but the only real way to prioritise for the organisation is to put the finding into the organisational context, and that requires not just the solid asset management you can trust but also enterprise architecture and business process modeling, IT service modeling and impact assessment done in advance and repeated on schedule, etc. You need to know your organisation really well to be able to tell if that's the right log4j [author's note: Java-based logging library] to spend time on.

End of Interview

Appendix 6 – Interview Transcript: Python Programming Teacher

Interviewee (Teacher A): ANDREI LUNJOV, 30+ years in programming, including 2 years as a programming teacher at school
Position: Software Architect, Estonia
Interviewer: Anastasiia Shapran
Date: 01 May 2025
Duration: 30 minutes
Language: English (translated from Russian)

Interviewer (I.) Have you ever worked in a school before?

Teacher (T.) No. This is my second year.

I. What did you encounter when you started teaching? Were there difficulties in making the curriculum and fitting lessons into your work schedule? Did you take any extra teaching courses?

T. Extra lessons in the schedule are always inconvenient, especially at the time they're on the school timetable. Well, what can we do? I was offered to teach lessons because they couldn't find anyone else. About the teaching courses - I haven't taken any, and I think people are independent enough in the last years of school that I don't need to deal with any psychological aspects.

I. When you met your students, was there a conversation about why they came to your course? What were they expecting? Have they had experience before?

T. With one class, it would have been unnecessary; the students came because it's in their programme. With the second class, there was a section of very motivated students. A few guys could do something, more able to do it. My intention was not just to take the tasks and solve them, but to show a more interesting side of the question.

I. How often did you include cybersecurity-related tasks in your programming lessons?

T. Well, honestly, I was only interested in cybersecurity as a provider of interesting tasks.

Cyphers provide a good set of programming dictionary problems, including brute-force solving and different heuristics for solving. That's my view of cybersecurity. They were interested, so I told them about the public key and even touched on some number theory. I didn't look at security itself; it's just one of the reasons for me to do some programming.

I. Did you and your students guess passwords?

T. Yes, he [author's note: cybersecurity teacher] suggested it to me, and I thought, why not? We encrypted something initially, then we picked some passwords, simple cyphers. In the end, I picked up a substitution cypher, considering that we know the language of the message. Then I went into a more interesting area, the Cretan letter, Linear B. I told them how it was deciphered. I offered them a task to do it themselves to decipher the linear letter B. But nobody took it up. I wanted to show them myself, but didn't have time either. But at least I told them how it was roughly done.

I. What were the students' difficulties?

T. Among the difficulties in one class were unwillingness to learn, reliance on Chat GPT, and a low level of programming knowledge itself. In another class, everyone had a different level and ability to program and a different speed to get the information. Well, I hope there's something left.

I. Did you give them homework?

T. Of course. Our course was structured so that we solved some simpler tasks in class. I gave them the task in the form of a discussion, and I asked questions. They all tried small tasks, and I gave a more complex task for the next lesson.

I. What do you think if a student who doesn't understand programming very well uses Chat GPT, prepares at home, parses, and comes to your class prepared? Is it bad?

T. No, if he uses Chat GPT and aims to understand - thank goodness. But if he brings me an assignment and can't answer a single question on that assignment, I have a hard time hiding my squeamishness. Why did a man come to the gymnasium if he didn't want to think?

I. What approaches have helped you to explain complex topics to your students? Did you use project work or group work in your lessons?

T. I needed each student to develop individual skills, even if not very much. There was a part of the assignment for group work. I tried to encourage communication between them. Well, as always, someone is interested in discussing with others, someone needs to do it for a tick. I tried not to load them because of the state exams period.

I. Maybe you have heard that a couple of years ago, in Estonia, a programming school appeared [author's note: *«Kood/Jõhvi»*], where participants learn and follow the programme without any guidance from teachers. There is a platform with tasks, internet access, and classmates. What do you think of this format?

T. I started programming in 1988, and nobody taught me. I don't think you can learn programming when someone teaches you. You can give some initial steps. You can show something to a person, open something, or provide advice. But 95% of learning is done by yourself, that is, in general. I do not treat programming, in Aristotelian terms, as *artes serviles*, i.e., servile crafts. I consider it *artes liberales*, i.e., liberal or free art. And a person does free art because he is interested in it. Suppose a person wants to do something because he heard programmers get paid a lot. And that's why he decided to... I don't need such a colleague; I don't share this view.

I. I see. You wanted to present information during the lessons so students could absorb as much knowledge as possible, right?

T. No, that's too easy. My task was, in Lacan's terms [author's note: *Jacques Lacan* (1901-1981) – French psychoanalyst], if I may say so, to infect with *enjoyment*. I aimed to convey the experience of *enjoyment* — in other words, to present programming as a form of free art.

I. Did you succeed, do you think?

T. I initially overestimated their level in the first case with one class. It was my first year as a teacher at school. I didn't know what the level was. I didn't realise that derivatives were only taught in the 11th grade or so. I didn't know that they don't get integrals. And also, some strange self-confidence, a lot of weird problems. That's why I had a harder time teaching in that class. In another stronger class, it was successful. And I tried to show more classic computer science. In the end, those who did not know how to program before the course solved the tasks. They were almost equally difficult for these students and those students with programming experience. Because it was not exactly applied, but we look at issues in a more complex way. We try to reason there. We try to understand algorithms and how they all work. Password brute-forcing and similar tasks helped in

this sense. There were also problems where the choice of data structure is critical for its solution, which is quite challenging to achieve with modern computer power. On the other hand, I approached as much as possible in Python to use a functional approach. And taught programming differently in general. The goal was not just to teach how to write an iterative programme like a monkey. We were formulating the problem at a higher level. At the core, if you have one, it is how you develop the end goal. That problem has been practically solved. That's the approach. There are students engaged, for example, in painting dots on the screen in different colours and writing some simple scripts, yet they think they already know how to program. It shocked them at first when they encountered the tasks I offered them. And then they started to learn.

I. What skills do you think are key for high school students in the context of programming and maybe cybersecurity?

T. I would label such skills: a willingness to learn, a way to look critically at your skills, the ability to realise that you don't know something, an interest in discoveries and learning new things, and the desire to work by following your interest. So basically, what a psychoanalyst would call enjoyment. Remember that test for little kids where they can have one candy now, but if they wait 10 minutes, they get two candies [author's note: In the 1950s and 60s, *Walter Mischel* conducted a study in Trinidad, examining children's ability to delay gratification across different social and cultural groups. These observations became the basis for the famous Stanford marshmallow experiment conducted later.]. This is a soft skill. This is life in the enjoyment category, the willingness to exert oneself to get results. If you do not have it, then, unfortunately, in the 10th-11th grade, little can be done.

I. You said that you had two classes. Both are in the IT profile?

T. I have two classes. The course is 2 years long. The current 12th and 11th graders have now taken the whole course.

I. What can you recommend to your students? Where should they start for students interested in working in the programming field?

T. One should not initially think about jobs and money. If a person immediately focuses on earning money and how much they can get for it when choosing an occupation, then it is unlikely that something worthwhile will result.

I. For how long should they not think about money?

T. Preferably for the whole life.

I. And the ability to sell oneself, let's say, and to value, to receive the appropriate means of subsistence. Are these soft skills?

T. Yes, but how does that relate to programming?

I. As well as to other spheres.

T. I advise referring to Aristotle's concept of Servile and Liberal Arts. Now, this kind of questioning is inappropriate when discussing the liberal arts. In that case, a person does what he is interested in. And the recognition of success will come in due time. Yes, recognition may or may not come - we can remember great artists, many of whom died in poverty. Human life is unpredictable, and programming is no exception. If a person puts money at the centre of his priorities, he will likely create nothing of value. If you move only to earn money in any field, the maximum you will get is money. There are people for whom money is not a means, but a goal and even a form of art. For example, financiers are interested in money not for the sake of spending but for the sake of money itself as an intellectual challenge. They have an almost selfless passion for it. Such people can achieve something. However, even for them, specific amounts are not of key importance. And if the aspiration is limited solely to the desire to earn money, you are unlikely to get anything but mediocrity. And this is the case in any field.

I. Thank you. Have you discussed ethics and programming in your classes? Can students, with their current skills, start abusing their knowledge?

T. Sure, we can all start abusing a little bit. And ethics is a personal issue for everyone. What's abuse?

I. Doing bad things. To join a more advanced student and write some code, do a little phishing attack. I mean, where's the line of legality and ethics? Did the students go through this in your classes?

T. Well, the court sets the line of legality. That's not my field. I'm interested in what's interesting.

I. Have you talked to your students about how code can be written more readable for another person?

T. On the contrary. Everyone writes the way they want, the way they like. Mass programming is not engaging; I get enough of it at work. It is a way of self-expression. I am an artist; this is how I see it. Accordingly, if I have written such a code and another cannot understand it, well, I won. There is such a practice that everyone should be kind and help others. That's not true. The real environment should be challenging and competitive, because these are adult games. So, you must strive, you must be motivated.

I. What would you do differently if you were teaching a course like this again?

T. I would add a few small tasks and issues from Chat GPT. I'm OK with the structure of the course. I'm satisfied with the second-year class. The only thing was that the same situation kept repeating: the code generated by Chat GPT looked monotonous. It almost always writes in an imperative style, especially if the question is not precisely formulated. The volume of this imperative and sometimes marginally usable code was overwhelming and challenging to deal with within the course. I have yet to think about how to work with it further.

I. Thank you very much for the interview. It was a pleasure listening to you and learning about the inner workings of a high school course.

T. Well, it's a very atypical course. I have an atypical view. I did this course to diversify my working life. I found it quite interesting, too. Good luck with your work!

End of Interview

Appendix 7 – Interview Protocol: Cybersecurity Teacher

Interviewee (Teacher B): IVAN, 22 years in IT, including 7 years in Cybersecurity and 1 year as a Cybersecurity teacher at school
Position: CIO, CISO, public and private sector, Estonia
Interviewer: Anastasiia Shapran
Date: 01 May 2025
Duration: 40 minutes
Language: English (translated from Russian)

Interviewer (I.) Did you come to teaching from the private sector? Is this your first experience working in a school?

Teacher (T.) Yes, I came from the private sector. However, this is not my first time working in a school. I've worked in supportive roles before and even participated in organising events for younger students.

I. What organisational barriers did you face (curriculum, scheduling, qualification requirements, etc.)? Do you take part in developing the program and materials?

T. There were no serious barriers. Although the course was new for me, I received great support from colleagues, especially the gymnasium principal, who introduced me to the format and shared helpful materials. I also consulted with other experts. I participate in adapting and developing the curriculum, assignments, and tests for the students.

I. What resources or materials are lacking?

T. There were a lot of materials, making it difficult to focus. What I lacked was a more structured set of case studies and interactive platforms for modelling attacks in a safe environment. A more refined toolkit would help ensure consistency and clarity.

I. What topics does the cybersecurity course cover, and what competencies should students aim to develop by the end?

T. The course covers basic cyber threats (viruses, phishing, malware), encryption, device and network protection, operating system hardening, secure communication, malware

detection, and secure data deletion. We use tools like Kali Linux. By the end, students should be able to secure their own devices, recognise threats, use encryption, and apply basic cyber hygiene and privacy principles.

I. What technical or soft skills are essential for high school students in the context of Cybersecurity?

T. Critical thinking, logic, and mathematical reasoning are essential. Also, curiosity, responsibility, and teamwork are key soft skills. Cybersecurity is a vast field, so adaptability and openness to learning are crucial.

I. Did you include programming in your cybersecurity lessons? How important is it for Cybersecurity?

T. Yes, in cooperation with the Python course instructor. We synchronised topics like encryption and hashing. Programming helps students understand how systems and scripts work. It's not always mandatory, but basic programming knowledge is extremely helpful in understanding cybersecurity logic.

I. What assignments or projects proved most effective or interesting for students?

T. Practical sessions were the most engaging, using Kali Linux, creating canary tokens, Wi-Fi password cracking simulations, and group work. Students also enjoyed guest lectures from industry professionals and group presentations where they taught their peers. I used Kali Linux mainly to give students hands-on experience with cybersecurity tools.

First, I showed them how to install Kali Linux, either on a virtual machine. I want to note that installing Kali Linux took the class some extra time. I explained that it's a system packed with tools for testing the security of networks and devices, but it should only be used with permission. Then we practised using some basic tools. For example, students used nmap to scan a network and find connected devices. They also tried Wireshark to see how data moves through a network, and Hydra to demonstrate how password attacks work, but only on test accounts we set up for the course.

I. How motivated are the students? What methods do you use to engage those who are less interested?

T. Motivation varied. Some students chose the course because they were genuinely interested, and others were attracted by the potential income in this field. I used gamified

lessons, open discussions, real-life examples, and peer presentations to engage all students, especially those who were less motivated.

I. Do you discuss the ethical aspects of Cybersecurity? Is there a risk that students may misuse their knowledge?

T. Yes, we discuss ethics from the start, including real cases and legal consequences. We make an informal agreement not to misuse knowledge. While risks always exist, I believe most students understand the responsibility that comes with this knowledge. The goal was to help them understand how a hacker might think, so they can better protect systems. We also spent time discussing ethics. It was important for them to know that using Kali Linux is only okay in a legal or educational setting. Hacking into someone's Wi-Fi, for example, is a crime, and I made that very clear.

I. Have your students encountered social engineering? How useful is it to teach this topic in school?

T. Yes, especially via social media. Social engineering is highly relevant, and understanding it helps students safely communicate online and in daily life. It's one of the most important and applicable topics.

I. What roles do parents and school administration play in fostering a cybersecurity culture at school?

T. A major role. Students should share what they've learned with their families. I plan to involve parents more directly next year through presentations and discussions. For example, to organise an event as a lecture where students will talk about what they have learnt. Do it in lecture format for their parents or other classes. With administrative support, we can extend Cybersecurity awareness beyond the classroom.

I. What would you change if you were to teach this course again? What practices or methods would you like to implement in the future?

T. I'd like more teaching hours to include CTF competitions, use cloud-based labs (e.g., TryHackMe, Hack The Box), and offer certification tracks like CompTIA. I'd also incorporate more legal/regulatory context (e.g., GDPR).

I. What would you recommend to students who want to pursue programming or Cybersecurity?

T. Do it because you enjoy it, not just for money. Passion, curiosity, and persistence matter. Attend meetups like RIA Cyber MeetUp [46], engage with online platforms, and seek internships. Those who are truly motivated and excited about the field succeed.

End of Interview

Appendix 8 – Interview Transcript: Gymnasium Principal

Interviewee (Education Expert): OLEG SHVAIKOVSKY, 28 years in IT, including 13 years in the Education sector
Position: Co-founder & Board Member at PÜHA JOHANNESE KOOL, Tallinn, Estonia
Interviewer: Anastasiia Shapran
Date: 01 May 2025
Duration: 30 minutes
Language: English (translated from Russian)

Interviewer (I.) You have over 28 years of experience in the IT sector, including programming, sales, telecom, a series of management positions, and experience as an EdTech investor. You are now a co-founder of the school, a physics teacher, and a mentor for the IT direction in the gymnasium. We will talk to you about gymnasium education, the shortage of staff in schools, cybersecurity and artificial intelligence in education, and the challenges facing the school community. How does the school determine the study directions for the gymnasium? What profiles does your school have? **Expert (E.)**There are four directions: Word and Culture, Form and Design, Nature and Human, and Data and IT. Why did we decide to launch exactly four profiles? It is a long story; we brainstormed for quite a long time. Several parameters have to come together: what is there and what might be interesting on the market, who can you find as teachers? There is, for example, "Word and Culture", the direction was born thanks to the idea of one of our employees; in fact, she made the programme for this direction. We have four directions in total, two humanities and two STEM, and we held this brainstorming 4 years ago, a year before the gymnasium opened. The school is now 13 years old, and this year will be the first graduation of gymnasium students. After discussing these areas in general terms and what they would be about, we were looking for people who could lead these areas as mentors.

I. Why didn't most people go into a trendy direction like IT? How was the division into directions made?

E. We agreed to take 16 students in each class from the beginning. So, one stream is 64 students. We have a humanities track and a STEM track, and they have slightly different curricula; for example, my favourite is physics. There is more physics in the science track, and we move faster with physics in the programme. Moreover, because there are 16 students in each class, there is more and more competition for entry into the IT profile. For

example, in the 3rd stream, i.e. 10th grade, we already have 19 students rather than 16, and we could have got many more. It is a pity that we have to say no to strong students, as there are no more places in the class.

I. Does the gymnasium have a pool of compulsory subjects and elective courses?

E. In our gymnasium, there are 4 pools of subjects. 70 courses in three years are compulsory in the state programme; this is stated in the Law on Education [author's note: (link) RÕK]. The second pool is the school choice, i.e. there are 10 subjects that our school has chosen as compulsory, for example, Christian anthropology, Greek language, Latin language, and so on. Then there are 15 courses related to the direction. And then there are 2 courses that students choose themselves. We allow more than two courses. In fact, more than half of the students take three to six courses. According to the Estonian Education Act, at least 97 courses must be completed in 3 years in the secondary school.

I. How is the programme for an IT class drawn up? What were you guided by?

E. I, as a mentor of the IT profile, came up with the idea, consulted with specialists and developed the programme.

I. Do you feel there is a shortage of qualified teachers?

E. In that sense, we are a lucky school; we don't have that. But in Estonia, it is a big problem. We actually have several candidates for almost any competition we announce. In the whole history of the school, in these 12 years, I can count on the fingers of one hand the times when we had a real problem finding a teacher. The school has a good reputation, and teachers want to come to work for us.

I. This year will be the first graduation of the 12th grade in your school?

E. Yes.

I. Where and how do you find teachers (e.g. IT profile-connected subjects: programming, cybersecurity, metathinking, etc.)?

E. In general, finding teachers is difficult. We were recently looking for physics teachers. There is very high competition among schools when looking for teachers, even tougher than in the IT industry.

I. How do you retain teachers in the long run?

E. It's such a multi-layered story. Well, in our particular context, we don't specifically pay salaries more; we pay as much as any other school. But we have the number of compulsory hours and the teacher's workload. In Estonia, on average, a teacher works 35 hours; our teacher spends 20-24 hours speaking in front of the class, and the rest is allocated for preparing lessons, checking pupils' work, i.e. pre- and post-processing. Anything above that is considered overtime and is paid separately. But the most important thing is that it is easier for a teacher to work in our school to a certain extent. For example, in a public municipal school, there are quite often misunderstandings between teachers and parents. Because parents frequently have the attitude that "I brought my child to you for 8 hours, for outsourcing, and now it's your problem". There are a lot of memes on the internet about this topic. Do you realise how much the attitude towards school has changed? In the past, if a teacher gave a low grade, it was the student's and parents' problem. Now it's the teacher's problem. However, we have very few misunderstandings between parents and students, or between parents and teachers, partly because we are a classic community school. We once had a problem finding a history teacher; it was a critical issue. At that moment, it turned out that one of our parents, the editor-in-chief, a historian by education, agreed to teach history lessons. And so, he taught lessons for 1.5 years. The children still remember that time with great fondness, because they saw their parents in a completely different way. We realistically have a lot of parents who are contributing to the school. I know a few more such parents who are qualified and teach at our school.

I. Are you open to cooperation with universities, IT companies or experts to develop or teach elective courses?

E. Yes, we are open to cooperation. For example, at TalTech, there is one course going on right now where our students come to the lab and do certain experiments. Next week, we are going on a study visit to the software development company Helmes with the IT profile class, and we recently went to Microsoft Office with the 11th grade. Yes, it is a constant interaction.

I. Is feedback collected from students on optional or elective gymnasium subjects? In what format? What is the impact of this?

E. Yes. It is a compulsory part of our school, one of the features that even other Estonian schools come to study, and we have been doing it since the very foundation of our school. Students write on a particular form and give the teacher and subject feedback. Then the teacher gives feedback to the students, and so on. This can influence the change of the

subject curriculum. However, we did have a situation once where we did not continue with the teacher the following year due to the feedback. He is a fantastic professional in his field, but he was not suitable as a teacher for the school. This is an isolated case. However, feedback is critical and allows us to change the next school year for the better.

I. Is the programme for different areas of study at the gymnasium drawn up over several years? Will the course "Cybersecurity Fundamentals" be offered next year as well?

E. Yes, the programme is drawn up over several years. After the course, we analyse what should be done differently, whether we should change the subject study plan or teach the lessons slightly differently. We have cybersecurity for the first time this year. It will also be taught next year.

I. Can the teacher shortage problem be partially solved by introducing AI?

E. Yes and no. Today, from the perspective of 3-5 years, no. As someone who is also involved in the TI-Hüpe project [author's note: AI Leap], I believe AI will not replace the teacher, but it can lead to 2 critical consequences. One, a more personalised approach to the student emerges, and two, you might increase the number of students per teacher. So, in that sense, there may be a little bit of help with teacher shortages. But it's not today's issue; it's a few years away. You have to go through several steps. We can talk for hours on this topic.

I. Could three or four subjects be overseen by a single AI supervisor instead of multiple teachers in high school, using pre-approved lesson plans and an AI-powered learning platform?

E. I don't believe in it. Everyone has a different point of view. I think it's wrong, it's not going to happen.

I. What perspectives of AI-Leap do you see as a teacher and representative of the gymnasium management?

E. I am very optimistic. You see, I am not very objective in this case, because I am one of the board members. And we are talking at this time, not before. As someone who is not objective at all, I think that artificial intelligence in the education system in general is probably the most serious game changer in the last 100 to 200 years. Full stop. Neither the internet, nor the pocket calculator, nor encyclopedias have been such serious game changers. It's probably comparable to the moment when printing came along. The moment

when Socratic conversations were replaced by a different model of education, when books became mass-produced and cheap. AI will play roughly the same role now.

I. What should be done so that the student doesn't just bring in a ready-made piece of work done by AI, but actually engages in thinking?

E. Yes, I understand what you are saying, we need to change the whole concept of lessons. For example, I can say that the classical conventional homework has lost all meaning. Yes, this, among other things, leads to the fact that we need to change the methodology. At our school, I teach physics according to the so-called flipped classroom principle, which is when a student comes to class with an understanding and we emphasise practice. That is, there is no point in trying to use any tools to catch plagiarism. We need to build the process in such a way that the student uses artificial intelligence and learns at the same time. Because the biggest problem that arises, the biggest danger of artificial intelligence, is that there is a natural temptation to outsource the thinking process. Let it do the thinking for me. That's what the school has to fight against and, accordingly, build the process in such a way that the student is not tempted or required to do that.

I. What has already changed in the school now with the advent of AI?

E. Well, I have already given you one example, many things have changed. We don't give classical homework in many subjects. We don't give home essay writing; it's written in class here. A lot of things have already changed, and this is just the beginning.

I. Informatics is now a subject of choice in basic school and in gymnasium. What is your opinion about the absence of informatics in the compulsory state curriculum?

E. You know, the question here is not about the subject, but about competence. That is, the question is that there is a certain digital literacy that a student (pupil) has to know at certain phases, and this is not only a gymnasium issue, i.e. some things are necessary in the 4th grade or in the 7th grade, for example, to work with tables. I am also in favour of not separating the subject of computer science, but weaving a certain amount of computer science into a regular subject. For example, in maths, pupils should use Excel and do something there, draw graphs or work in GeoGebra. That is what they do at our school. You see, it is not informatics as a subject that is important, but a certain digital literacy.

I. What is available to your school in terms of resources and technology to teach, for example, programming and cybersecurity?

E. Probably, you've talked to a cybersecurity teacher and a programming teacher already. Our school's fundamental approach is that we are full Google-domain customers for education—we use all the tools: Classroom, Drive, Docs, Sheets, and even Gemini. We have a full subscription for the whole school and use the ecosystem quite extensively.

I. How conscious are the children about their digital security? Have there been any social engineering incidents at your school?

E. I haven't had any mass incidents come to my attention, which could very likely mean that there haven't been any, but I'm just in case, I'm not going to claim. We're not talking about a separate cybersecurity lesson, which is what IT-Profile is doing now. I can show students in my physics class how I would build a prompt in Gemini, what the answer would be, and how it would be if the prompt were changed. It's a matter of how the teacher weaves it into their subject.

I. Where do teachers acquire those skills so that they can weave them into their subject?

E. This is an excellent question. It can be done either through centralised training or, if we are talking about Estonia, in general, it is very often related to how good the educational technologist (haridus tehnoloog) is in your school. We are lucky; we have a good educational technologist. In general, there are quite a lot of training sessions in Estonia, including for teachers. By the way, in this sense, it is good that Estonia has already developed and implemented the so-called competence model, i.e. what a teacher should know, which also includes the heading of digital competences. Another thing is, how much do teachers really know? Yes, this is a separate question. I mean, I know teachers from our school who are not very well informed. But formally speaking, this competence system for teachers is quite well thought out at the state level in Estonia. There are trainings organised by HARNO (Estonian Education and Youth Board), usually video trainings.

I. The penultimate question. How can we teach cyber defence tools and avoid potentially dangerous behaviour? Does the school have a code of digital ethics?

E. We don't have a formal code of digital ethics in our school. But I believe that we need to teach through live communication, internal seminars, and the exchange of experience. By the way, our educational technologist, whom I mentioned earlier, has such a series. Once a fortnight, there is a seminar where teachers voluntarily discuss different topics and share their approaches. It's very effective.

I. This is the last question. From the point of view of school administration and as a

teacher, what do you see as “growth areas” in education, and what topics would you like to draw the attention of the school community to?

E. Reaching out to the school community is a topic that takes several hours. One of the problems is that there is a wrong image of a teacher in society. That it’s hard and poorly paid, which is also true. But somehow, there’s a lot of talk about that negative part. Not much is said about the positive part. Roughly speaking, no matter what crises exist in the country, the teacher’s salary in Estonia is already higher than the average salary in the country and is slowly growing. So, it’s like the government’s plan that in the next few years, I think by 2028, teachers’ salaries will be 120% of the average salary in the country and so on. There are other pluses, quite big ones, you know, that somehow aren’t talked about. The minuses are talked about, and as a consequence of this case, young people do not want to go to work as teachers. The image of a teacher has to be changed. And the growth area, the most crucial, serious topic in the whole Estonian education system right now, is this quiet artificial intelligence. This is the most important topic, which one group of good, intelligent people is working on very intensively.

I. Thank you very much for an interesting conversation. Let’s hope it goes well, and we will jump high!

E. Thank you!

End of Interview