TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Timofei Mihhailov 221935IVCM

DEVELOPMENT OF CYBERSECURITY LEARNING MATERIAL FOR FUTURE AND CURRENT SCHOOL TEACHERS IN IDA-VIRUMAA

Master's Thesis

Supervisor: Kaido Kikkas
PhD

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Timofei Mihhailov 221935IVCM

KÜBERTURVALISUSE ÕPPEMATERJALI VÄLJATÖÖTAMINE IDA-VIRUMAA KOOLIDE TULEVASTELE JA PRAEGUSTELE ÕPETAJATELE

Magistritöö

Juhendaja: Kaido Kikkas
PhD

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: Timofei Mihhailov

16.05.2025

Abstract

Cybersecurity education is increasingly recognized as an integral part of a modern education system, ensuring that learners have the knowledge and skills to operate safely in the digital environment. However, integrating cybersecurity into school education poses a significant challenge, especially for educators who lack specific training in this area. This research responds to this need by focusing on the development of specific cybersecurity educational materials tailored for current and future school teachers in Ida-Virumaa. The research will be based on a review of existing Russian-language cybersecurity materials, pedagogical approaches, and best practices. The study will use a mixed-methods research methodology including pre- and post-training surveys. Based on the data collected, a structured curriculum will be developed that addresses key concepts of cyber security and includes teaching methods that can be adapted to different learning environments. Particular emphasis will be placed on the use of storytelling and interactive learning materials to increase teacher engagement and understanding of cybersecurity principles and practices. The effectiveness of the resulting learning materials will be evaluated in a pilot project in cooperation with local educational institutions. Feedback will be collected from participating teachers and analyzed for further improvement and enhancement of the curriculum. The results of the study support the development of cybersecurity education at the school level, with a particular focus on the Ida-Virumaa region, where a large part of the population is Russian-speaking. The aim of the initiative is to support the growth of teachers' digital literacy, strengthen their resilience to digital threats, and create an educational environment that fosters awareness and safe behavior in the digital world.

Keywords: cybersecurity education, teacher study, teacher training, cybersecurity awareness, cybersecurity at school, digital literacy, storytelling, interactive learning, minority language, scenario-based education.

This thesis is written in English and is 50 pages long, including 8 chapters, 12 figures and 1 table.

Annotatsioon

Küberturvalisuse õppematerjali väljatöötamine Ida-Virumaa koolide tulevastele ja praegustele õpetajatele

Küberturvalisuse alane haridus on üha enam tunnustatud kui kaasaegse haridussüsteemi lahutamatu osa, mis tagab, et õppijatel on vajalikud teadmised ja oskused turvaliseks tegutsemiseks digitaalses keskkonnas. Küberturbe temaatika lõimimine keskharidusse kujutab endast aga märkimisväärset väljakutset, eriti nende pedagoogide jaoks, kellel puudub sellealane eriettevalmistus. Käesolev uurimistöö vastab sellele vajadusele, keskendudes spetsiaalselt küberturvalisuse õppematerjalide väljatöötamisele, mis on kohandatud Ida-Virumaa koolide praegustele ja tulevastele õpetajatele. Uuring põhineb olemasolevate venekeelsete küberturvalisuse materjalide, pedagoogiliste lähenemisviiside ja parimate tavade läbivaatamisel. Uuringus rakendatakse segameetodil põhinevat uurimismetoodikat, mis sisaldab koolituse-eelseid ja -järgseid küsitlusi. Saadetud andmete põhjal töödeldakse välja struktureeritud õppekava, mis käsitleb küberturvalisuse põhikontseptsioone ning sisaldab õppemeetodeid, mida saab kohandada erinevatele õpikeskkondadele. Erilist rõhku pannakse jutustamise ja interaktiivsete õppematerjalide kasutamisele, et suurendada õpetajate kaasatust ning mõistmist küberturvalisuse põhimõtete ja praktikate osas. Valminud õppematerjalide tõhusust hinnatakse koostöös kohalike haridusasutustega läbi viidava pilootprojekti käigus. Osalevatelt õpetajatelt kogutakse tagasisidet, mida analüüsitakse õppekava edaspidiseks täiendamiseks ja täiustamiseks. Uuringu tulemused toetavad küberturvalisuse hariduse arengut koolide tasemel, keskendudes eriti Ida-Virumaa piirkonnale, kus suur osa elanikkonna emakeel on vene keel. Initsiatiivi eesmärk on toetada õpetajate digipädevuse kasvu, tugevdada nende vastupanuvõimet digiohtudele ning luua hariduskeskkond, mis soodustab teadlikkust ja turvalist käitumist digitaalses maailmas.

Märksõnad: küberturbeharidus, õpetajaõpe, õpetajakoolitus, küberturbeteadlikkus, küberturve koolis, digitaalne kirjaoskus, jutuvestmine, interaktiivne õpe, vähemuskeel, stsenaariumipõhine haridus.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 50 leheküljel, 7 peatükki, 12 joonist, 1 tabel.

List of Abbreviations and Terms

2FA	2 Factor Authentication
ADDIE	Analysis Design Development Implementation Evaluation
CTF	Capture the Flag
K-12	Kindergarten to 12th Grade (primary and secondary school)
NCSC	National Cyber Security Center
NCSC-EE	National Cyber Security Center Estonia
PC	Personal Computer
PDF	Portable Document Format
RIA	Republic of Estonia Information System Authority
SAM	Successive Approximation Model
SSL	Secure Sockets Layer
STEM	Science, Technology, Engineering, and Mathematics
URL	Uniform Resource Locator

Table of Contents

List of Figures

List of Tables

1. Introduction

This section will introduce the problem statement and research design, containing motivation, research problem, scope and goal, research methods, and thesis organization.

1.1 Scope and Goal

The motivation for writing a thesis on this topic is to improve both schools basic education and general secondary education levels (1-12 classes) teachers' cybersecurity capabilities, skills, and awareness in Ida-Virumaa region of Estonia. Estonian education system can be seen using here[1]. Providing that group with training in the cybersecurity field is vital to prepare teachers for today's cyber threats and evolving technology around the teaching process. By introducing teachers to vital cybersecurity topics, it would be possible to raise interest in cyber overall. Making that change is essential to increase the cyber defense of public schools in Ida-Virumaa.

Cybersecurity training programs should be specifically designed to address the distinct needs of educators. The majority of these initiatives focus on preparing school teachers to effectively deliver cybersecurity education to their students. To fulfill this role, it is imperative that teachers themselves attain a foundational level of cybersecurity literacy. Accordingly, the provision of comprehensive, up-to-date training in the educators' native language is essential. This is particularly relevant in regions such as Ida-Virumaa, where a majority number of people are native Russian speakers. Delivering training in the mother tongue not only facilitates this linguistic transition but also contributes to a more secure school environment. Furthermore, it strengthens educators' cybersecurity competencies, thereby broadening access to digital tools that enhance the quality, interactivity, and safety of the educational experience.

In 2024 Estonia started to transition education into Estonian-only in schools. It is a first step in transition which includes kindergartens and basic school only (1st to 4th grade). This transition step will last until 2030. At the moment of writing this work, this step does not involve additional requirements from teachers with a higher proficiency level in Estonian as C1. Ida-Virumaa is recognized as most trouble state with this transition and offered all required needs to make the process more smooth. Estonia aims to shift all education in Estonian based only in the future. Unfortunately, this shift will not happen

[1] https://www.educationestonia.org/about-education-system/

fast and the cybersecurity of teachers in Ida-Virumaa is needed today. That is why this work aims to create targeted interactive cybersecurity material in the native language of the majority of Ida-Virumaa Russian speakers. [1]

Providing that group with knowledge in the cybersecurity field can also increase the interest in cyber education among teachers. By motivating teachers to be aware of current cyber threats and problems, it would be possible to translate their knowledge and interest to their students and peers. Increasing interest in the field from a young age can provide enough people interested in cybersecurity to the workforce afterward.

The results of this study can be transferred to other teacher group minorities within any country that has a similar situation to Ida-Virumaa in Estonia (the majority of teachers are native speakers of a language other than national). Also, the effectiveness and engagement of the method chosen to produce interactive learning material could be used if proven effective.

The main aim of this study is to create training material for the school teachers that would not require previous cybersecurity-related training.

Scope of this study:

- Measure cybersecurity awareness of currently working Russian-speaking school teachers of Ida-Virumaa
- Identifying current problem areas in cybersecurity education of this teachers group
- Development of gamified learning material, which will be based on educators' needs, threats mentioned in the literature, and cyber-incidents of cyberattacks on schools that happened previously
- Assessment of training material results

Limitations are:

- Constraints in the availability of data for Ida-Virumaa school teachers' cybersecurity awareness
- A relatively small sample size for awareness assessment
- A restricted number of participants available for testing the developed training materials

Key assumptions:

- Teachers are interested in improving their cybersecurity skills and awareness
- Assumption of varied learning styles
- Basic computer literacy of the targeted group
- Providing training in native language would increase effectiveness
- Lower level of cybersecurity awareness within school teachers of Ida-Virumaa group due to restrictive access to trainings conducted in other languages

Providing teachers with practical and useful learning material in a school environment is a challenging task but necessary one. By researching that topic, it would be possible to assert and understand which skills teachers currently lack and improve them by creating gamified learning material in an online environment.

1.2 Research Questions and Methods

This thesis investigates the need for particular essential cybersecurity training by looking into current research on cybersecurity skills required for school teachers.

By creating tailored training material in the Russian language this thesis aim to improve awareness and defense against current cyber threats, as a lack of educational material tailored for school educators exists. Training is available for teachers in Estonian and English, but Estonia offers limited training for the Russian-speaking majority of the Ida-Virumaa region. The majority of cybersecurity learning material is provided in the Estonian language. This issue is relevant as Ida-Virumaa is currently in the transition stage of moving to use the Estonian language. Educating in the Russian language would increase the effectiveness and readiness of Ida-Virumaa teachers to stand against cyber threats. Doing that research will help prepare school educators to face today's cyber challenges.

The research questions to guide this study are:

- What are the specific features of cybersecurity training for school teachers in Ida-Virumaa (in the context of the Russian-speaking majority and lack of cybersecurity education in this language)?
- What teaching methods or pedagogical approaches effectively convey cybersecurity concepts to Ida-Virumaa school teachers?
- What cybersecurity resources (e.g., training materials, workshops, online courses) are currently available for school teachers in Ida-Virumaa?
- Which cyber threats are most dangerous and should be prioritized? What topics (e.g., safe internet practices, data privacy, threat awareness) should be emphasized?
- What level of preparedness do they currently have to address cyber threats (in the

context of the Russian-speaking majority and lack of cybersecurity education in this language)? What could be done to improve preparedness?

Research methods that will be used:

- Mixed-methods pre-training survey to measure the current level of awareness and understand threats that need to be addressed among school teachers
- Mixed-methods post-training survey to understand problem areas in learning material design and effectiveness of methods or pedagogical approaches chosen

Pre-training will be done on focus groups interested in improving their knowledge and awareness level in cybersecurity. This study will help identify which particular skills are necessary for current and future school teachers and understand the cybersecurity threat cases they face during their work activity.

After training, by providing learning material to the focus group, this study aims to conduct a mixed-methods post-training survey to measure engagement, interest, and study results. Besides measuring improvements in cybersecurity awareness, this study's goal is to ask for future enhancements to continue improving the quality of this learning material.

1.3 Novelty and Contribution

A review of the literature on this topic indicates a clear need for instructional materials specifically designed for school teacher groups. Primarily, studies encountered were aimed at high school or information technology student's cybersecurity capabilities; some of such studies can be seen in [2, 3, 4, 5]. Creating an experience aimed at teachers' groups would make it possible to create tailored material specifically for them. Focusing on teacher's attitudes and motivation is crucial to creating an experience that best fits teacher's needs. Understanding barriers to adopting such programs in a school environment is essential to generate comprehensive results and improve school cyber posture.

Despite the availability of a few cybersecurity training tailored for school educators, teachers are still not prepared enough to fight the evolving cyber threat landscape. Therefore, there is a need to produce more gamified learning material for school teachers of Ida-Virumaa in their mother language, which is Russian.

This study aims to create engaging and effective learning material that can be studied by future and current Ida-Virumaa school teachers. The proposed solution would leverage the usage of gamification techniques, storytelling, and other interactive methods to enrich

usage and interest teachers in exploring modern cybersecurity challenges and see proposed solutions to solve them. By making that change, it would be possible to raise awareness, skill, and interest in cyberspace. This change can lead to an increase in the number of educators conducting a class on cybersecurity for their students, or transferring knowledge to their peers.

Contribution to this thesis work is threefold. First, the current cybersecurity awareness of the Ida-Virumaa school teachers working in a public school environment will be measured. Secondly, creating gamified learning material to help teachers improve their cybersecurity readiness, knowledge, and awareness. Thirdly, in this thesis, work analysis will be done regarding the effectiveness and engagement of training material by asking teachers to complete a survey after completing the learning material. By making such a contribution, improving knowledge in the ever-evolving cyber domain in public schools would be possible.

1.4 Thesis Organization

This thesis starts with the "1. Introduction" section. The first section of that chapter discusses the scope and goals, explaining both motivation and the primary end goal. After that section comes the "1.2 Research Question and Methods" section which explains all necessary primary and secondary research questions. This section will also explain methods used to answer those research questions and gain meaningful insights into Ida-Virumaa educators' cybersecurity preparedness. Next comes the "1.3 Novelty and Contribution" section information to answer the crucial question of why this research is important and how much work is going to be done to bring meaningful results to the current body of knowledge in that area. This section concludes with the current "1.4 Thesis Organization" section.

The second chapter of this work named "2. Background" contains all necessary information regarding the literature review and practical context to develop unique and practical learning material for current and future educators of Ida-Virumaa. The first section of that chapter, titled "2.1 Practical Context", explains both the language specifics of the region and the factors that led to their development. It concludes with a section on currently available cybersecurity education resources for educators of Ida-Virumaa in the Russian language. The second section of that chapter is "2.2 Literature Review" containing crucial information such as:

- Why cybersecurity training for educators is important?
- Why teachers are a crucial part of student cybersecurity awareness?

- Methods used in previously created learning materials for educators
- Examples of training materials implemented and documented in the literature
- Current threats for educators within school environment

The third chapter of this work, titled “3. Methodology”, provides essential details about the implementation phase of learning material creation. It covers pre- and post-training surveys, including the tools and resources used to reach the target audience, as well as the survey questions. This chapter helps readers understand the author’s decisions regarding the technology employed to develop effective learning materials for teachers in Ida-Virumaa schools.

The fourth chapter named “4. Pre-Training Survey Results” contains an analysis of the survey answered before training has been completed. This information is essential to understand the current landscape of Ida-Virumaa school teachers as there is no publicly available information regarding school teachers of this specific region. By following this chapter reader can see each section of questions in depth and gather insights for his future research.

The fifth chapter is “5. Learning Material Development” which contains data regarding development aspects of learning material for teachers of Ida-Virumaa. This chapter explains the contents of the material in detail and discusses the iterative nature of this particular training material developed using SAM [6] methodology.

The sixth chapter, named the “6. Results”, contains an analysis of an anonymous post-training survey. In this chapter, the reader could understand the effectiveness and engagement of training material developed within this thesis work. This chapter also answers primary and secondary research questions established in the “1.2 Research Question and Methods” section. Within that chapter, the reader could also find the “6.5 Future Work” chapter, which could help to gather insights into the development of similar study material in the future.

This work’s last chapter is “7. Conclusion” which contains a discussion of the work done and the effectiveness of chosen methods.

2. Background

This section will discuss both the practical context and the literature review. The practical setting is crucial for understanding the nuances of the Ida-Virumaa region in Estonia and for guiding future research. The literature review is essential for this chapter, as it presents existing studies relevant to the thesis topic. By integrating insights from both areas, it becomes possible to develop modern and practical learning materials.

2.1 Practical Context

For this work, it is essential to underscore language specifics of Ida-Virumaa and publicly available materials for cybersecurity education. This step is vital to introduce to the reader why learning material will be done in Russian and to avoid repeating any previously done material available online to the school teachers' group.

In 1945, Estonians were presented as 97% majority of Estonia's population. During the Soviet period, 1 600 000 people arrived in Estonia, from which 1 260 000 left, which yields a net migration of 340 000 people. This migration greatly affected Estonia's population, mainly between 1960 and 2011. In 1980, Estonia's population dropped to an average of 51% of Estonians, even lower in Tallinn (capital of Estonia) or cities in Ida-Virumaa. Migration from the Soviet period still affect the main population of Estonia in 2025, which creates specific difficulties with the transition into the Estonian language for Ida-Virumaa region. [7]

2.1.1 Ida-Virumaa Language Specifics

This section will describe why Russian is currently the most prevalent language for teachers in Ida-Virumaa.

In population census done on 31 December 2021, it is concluded that people with a command of Russian language living in Estonia overall are 878 782 people [8] out of 1 331 824 people overall [9]. 370 722 people out of this amount are native Russian speakers [9]. Ida-Virumaa's situation is different from that of the country as a whole. In Ida-Virumaa there are 110 255 (83%) [10] native Russian speakers out of 132 741 [9] region population. It is important to notice that only 35 980 (32%) out of 113 390 non-native Estonian speakers living in Ida-Virumaa can speak Estonian as foreign language, and only 27 130

(20%) out of 132 741 can use English [11]. Therefore, making training available in the native language of the majority in Ida-Virumaa is essential. Currently, some cybersecurity material is available for Russian-speaking groups, which is explored in the next section.

2.1.2 Training Resources Currently Available

This section is dedicated to a discussion of current education tools available related to cybersecurity teacher education. In this section, the author will assert cybersecurity material available in Russian. Materials analyzed in this section help to determine which tools/articles are currently available to avoid redundancy in future training material. Those materials are also essential to deciding on common issues for teachers within their work in public schools.

In video content provided by Chuiko Roman on youtube [12], learning material is created specifically for teachers and students. This video contains necessary information about basic cybersecurity. Topics covered in this video are:

- 2FA
- Cyber threat types
- Cyber threat vectors
- Password strength and management
- Web security, including forms and SSL protocol usage
- Windows password security

In "Cybersecurity for Teachers — What Should You Know in 2025?" [13] article, the most needed information for school teachers is presented. This article covers topics such as students being a threat, safe internet usage, and cyberbullying. This article also provides some guidance on how to lead cybersecurity education classes for students with examples. This article contains a lot of tips and action patterns that can be used in public school environments. Information presented in this article is also available in multiple languages and references some statistics on why a particular issue is essential.

On "itvaatlik.ee" [14] web resource located information which does fit any private person's PC and smartphone usage tips. This information is an excellent start to the first steps into personal cybersecurity skill enhancement. Unfortunately, this resource does not contain information that is particular to teachers within school environments. Still, teachers can use most of the advice given by "ITVaatlik" on this website to be more secure within the school. This resource includes short but very visual information that teachers can use about:

- 2FA
- How to recognize and react to phishing links
- Password strength and how to create secure passwords
- Privacy implications
- Safe behaviour on social networks

Also, “ITVaatlik” [14] resource contains quick tests after most of the material presented on it, which makes learning more interactive.

“TargaltInternetis” [15] website is an excellent resource to gather info for events where teachers can develop their cybersecurity knowledge. Unfortunately, this resource only has a partial translation of Russian, which can make it inaccessible to those who do not know English or Estonian. Most study information available in Russian on “TargaltInternetis” aimed at developing teaching programs in schools for students and not at developing teachers’ cybersecurity skills. This material is still useful for educators as it describes how to act in situations like cyberbullying and how to involve a web police if needed.

Republic of Estonia Information System Authority (RIA) [16] YouTube channel is also a great way to find translated Russian basic information regarding cybersecurity with subtitles. This resource compilation is rich in quality and accessible to novice users of PCs, as most teachers in schools are. By exploring this resource, teachers can be aware of the majority of problems that happen to them in the cyber domain and be prepared to act accordingly.

2.2 Literature Review

During the last five years, teachers have started to use more and more tools to improve student’s engagement and interest in the subjects they teach. Due to that fact, teachers are more exposed to cybersecurity threats, and they need to know how to work with data security and which tools to be on the safe side. Internet activity with the students causes teachers to share online data with third parties, which leads to potential data misuse for other means than education. Teachers need data protection and usage training to mitigate probable threats. Some schools implement service and tools lists that comply with security measures like the Hawaii State Department of Education to ensure that data is used correctly and deleted after usage in a certain period. Unfortunately, teachers still lack cybersecurity education and thus cannot educate their students well in this field [17]. [18]

More schools are switching standard education methods towards smart education. Smart education is a complex of measures that are intended to bridge the gap between learned

and educator with the use of technology. Such technology can be generative artificial intelligence chatbots, smart boards, or the usage of different computer applications within the education environment. Smart learning environments enhance the learning experience using modern-age tools to upgrade the learning experience and accelerate it. [19]

2.2.1 Need for Cybersecurity Training

This section of literature contributes to establishing the way and type of training needed currently for school teachers. Conducting research on studies related to authors contribution goal is necessary to determine the main aims and motivation to educate cybersecurity teachers in public schools.

"Cybersecurity education and skills training is an unavoidable endeavor for all federal, state, and private organizations" cited from "K-12 Cybersecurity Education, Research, and Outreach" statement shows that cybersecurity education is essential for public schools to protect from cyber threats, especially those from state actors. There is a need for more qualified teachers who would be literate in cybersecurity and be able to teach their students key cybersecurity concepts. [20]

In "K-12 Educators' Self-Confidence in Designing and Implementing Cybersecurity Lessons" [21] article, perception and understanding of cybersecurity were explored while indicating a colossal need for teacher professional development related to cybersecurity awareness and education.

Research "Cybersecurity Education, Awareness Raising, and Training Initiatives: National-Level Evidence-Based Results, Challenges, and Promise" [22] indicates that the government must advance cybersecurity training for teachers. A national survey conducted by EdWeek Research Center [23] found that most school teachers need the opportunity to get cybersecurity resources in demand. Moreover, rural lower economic status schools also do not have such resources available, which was reported by 80% of school teachers [24].

Article "A University's Developmental Framework for Creating, Implementing, and Evaluating a Cybersecurity Micro-Credential Course for K-12 Teachers" [24] also indicates that there is often a combination of a need for more teaching knowledge and resources for school teachers to be cybersecurity literate. Research done by Mugayitoglu et al. indicates that some teachers became so-called "teacher-leaders" who have spread information gathered in the learning material organized in this study to other teachers. This finding shows that educating one school teacher can spread information and raise interest in cybersecurity among other educators.

In “Risk and Protective Factors for Intuitive and Rational Judgment of Cybersecurity Risks in a Large Sample of K-12 Students and Teachers”, school education was discovered while maintaining a balanced focus on both protective and risk factors of cybersecurity. Cybersecurity risk severity can be categorized as low, medium, high likelihood, and low, medium, and high impact. Given the prevalence of using technology among teachers, cybersecurity risk can be stated as high, while the impact is indicated as large. The significant impact in schools is characterized by the number of young cyber users vulnerable to cyberattacks and how critical technology is for the learning process. To avoid cybersecurity risk, one can use rational and intuitive judgment as stated in [25]. While rational decisions can be improved using cybersecurity education and awareness spread, some people rely heavily on intuitive ones. [26]

2.2.2 Cybersecurity Education Methods

Five primary education methods are based on the Delphi method in the article “Modeling Effective Cybersecurity Training Frameworks: A Delphi Method-Based Study” [27]: conventional, online, game-based, video-based, and simulation.

Article “Interactive Environment for Effective Cybersecurity Teaching and Learning” [4] suggests using game-based or simulation methods to achieve the best education results due to the ability to involve participants and develop teamwork skills. Gamification methods are more attractive and enjoyable than traditional ones, as stated in [4].

The study “Empowering K-12 STEM Educators: Enhancing Cybersecurity Awareness Through Professional Development” [28] contained information regarding the training of educators in cybersecurity awareness. This study uses a flipped classroom learning method, which includes watching an introductory video of the topic for 20-30 minutes and then receiving hands-on exercises. This method is beneficial in introducing new areas of cybersecurity to educators that they have never faced before.

The article “Cybereducation in Society — Benefits and Threats” [29] states that educators should incorporate the “four c’s” method into cyber education according to cyber experts. Those four methods are critical thinking, communication, cooperation, and creativity. Those methods are essential to implement due to the changing nature of cyberspace. Incorporating such methods would benefit the educational goals of educators, which is to upgrade their cyber skills for future in-school threats.

The article “Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes” [30] describes cybersecurity teaching methods, such as:

- Problem-based learning
- Project-based learning
- Hands-on learning
- Experiential learning
- Flipped classroom model
- Case-based learning

Those methods can be seen in the majority of university curriculum classes, which means that they prove their effectiveness. Teachers can use such methods within multiple domains of a problem and tackle the problem from different angles. By using methods like "problem-based learning" it would be possible to introduce a person to concrete problems that other people have experienced and provide a way to solve them. "project-based learning" is a way to tackle problems over time while using real-world tools. The "hands-on" is a method of education within a controlled study environment that provides knowledge on how to use tools within such an environment. The "flipped-classroom model" is a method where a person receives lecture materials ahead of practical class sessions, which helps people to study in their phase. Case-based learning is essential to show real-world problems and try to educate people to be prepared for particular cases. Educators can use all those methods to create engaging and resourceful experiences for teachers to understand learning materials. [30]

Also, the article [30] divides the learning environment into scaffolding and barrier levels. Such differentiation means a system where education is split into level systems based on how much guidance is provided to the student and how easily accessible the learning material is to him. In this article, education environments are divided into such categories with examples:

- Low scaffolding, low barriers — minimal teacher guidance and self-directed online course
- Low scaffolding, high barriers — minimal teacher guidance and course in a remote town with limited infrastructure and resources.
- High scaffolding, low barriers — high level of teacher guidance or education support and beginner boot camp
- High scaffolding — high level of teacher guidance and advanced topic training program provided by tech company

As this thesis implies low scaffolding and low barriers, article [30] suggests prioritization of problem-based, project-based, and case-based learning method usage.

Gamification is a process of applying game design elements to non-game activity according to "Gamification of Education: A Review of Literature" article [31]. Some aspects of gamified experience are badges, points, leader boards, immediate feedback, achievements, status, story, and other game elements in non-game contexts to engage and motivate participants mentioned in "Why Mary Can Hack: Effectively Introducing High School Girls to Cybersecurity" [5] and work by Nah Fiona Fui-Hoon et al. [31].

Another method is the capture the flag (CTF) competition documented in the "Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions" article. CTF competitions are straightforward to implement due to the nature of assignments and also provide different levels of depth to adapt to user skills and experience. Many platforms use capture-the-flag functionality, for example, FbCTF, CTFd, HackTheBox, PicoCTF, and TryHackMe. [32]

Another type of challenge that can be done is phishing attack competitions, which are presented in "Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks" [33]. This training relies on real working mail accounts and a scoring system to determine who has discovered fishing emails faster. People are motivated to be good at the game by providing real-life benefits like Amazon gift cards. This study uses an experimental method while measuring the "Big Five" personality traits.

In the article "CyberEscape Approach to Advancing Hard and Soft Skills in Cybersecurity Education", the "escape room" challenge is presented, which can also be applied as one of the methods for gamified cybersecurity training. Escape-room challenges are mainly used to build critical thinking and problem-solving skills to increase collaboration and communication. Those skills are also crucial for teachers to make intelligent decisions when a crisis appears so that that method can be used for training. One of the approaches for capturing the flag competitions is to use the Jeopardy style by providing different tasks with points assigned to them so players can choose challenges for their level of competence. [34]

2.2.3 Implemented Workshops for Teachers

In the article "Empowering K-12 STEM Educators: Enhancing Cybersecurity Awareness Through Professional Development" [28], the author discovers procedures to implement workshops for 9-12 grade STEM teachers. This workshop lasted for 2 days and contained quite mature cybersecurity topics. This research highlighted that teachers think their school management needs to reconfigure remote access for school, as indicated in the better post-training survey. This workshop contained such topics:

- Cyber ethics, privacy, forensics, and investigation
- Cyber threats analysis: concept of cyber data
- Basic ethical hacking: what do hackers do through wireless/mobile networks
- Cybersecurity through games-based learning
- Securing networks, internet, the web/cloud, email accounts, detection, and protection with tools
- Social media security and educational tools for kids learning cybersecurity
- Blockchain, encryption-decryption, authentication passwords, multi-factor, and single-sign-on
- Cybersecurity frameworks, career, standards, and Metaverse

2.2.4 Students Cybersecurity Awareness

Teacher's cybersecurity awareness is essential, but it is crucial to remember that they are the primary communicators with children and teenagers.

"Cases of online fraud, cyber-bullying, racial abuse, gambling, and pornography" cited from "Relevance of Cybersecurity Education at Pedagogy Levels in Schools" article are some factors of students internet use. These complex issues have been hard to control by the parents over the years due to rising complications and ease of use means to overcome restrictions set up by their siblings. Educators should promote and teach safe usage of the internet to youngsters in the school environment to prevent such cyber threats. [17]

Research "Why Mary Can Hack: Effectively Introducing High School Girls to Cybersecurity" indicates a need for more female representatives in the cybersecurity field, which can be solved by introducing cyber education in schools and trying to involve more female participants. Positive results are discussed in while organizing female-only education programs. [5]

2.2.5 Cybersecurity Threats in School Environment

"Phishing attacks are one of the most prominent forms of cyber attack today" mentioned in "The Human Factor in Phishing: Collecting and Analyzing User Behavior When Reading Emails". Those attacks, at their core, benefit from human nature, on one most prominent thing that humans will always make mistakes. Those mistakes can be either in decisions regarding specific actions needed or urgent actions to make. Many malicious users abuse those attributes in their attack execution phase. Phishing victims are usually lured into executing malicious attachments or manipulated to go to specially constructed phishing

websites. Constructing believable phishing messages is one of the main tasks of executing phishing attacks successfully. [35]

In most cases, phishing is an initial attack vector according to "2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)" [19]. Training to prevent school teachers from becoming victims is essential to prevent most cyber attacks within the school environment. European Union tries to fight this issue by providing training such as "Cyberphish"[1] which is unfortunately not widely spread, not available in the Russian language and not mandatory to complete for educators.

The scientific literature regarding phishing shifts from noticing concrete objects (for example, images, text, links) to more human-related properties (for example, persuasion, cognitive vulnerabilities) [35]. One of the phishing attack types present is smishing and vishing [36].

For a successful phishing attack, malicious users should first gain their victim's trust and lure them by using it to do particular actions discussed in "Don't Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review". Therefore, executing phishing attacks on public schools is more trivial as trust is one of the cornerstones of such public properties. As stated in the article, some user-specific properties make victims susceptible to phishing attacks: technicality, trust in technological solutions, risk awareness, and commitment level. Those properties are those of teachers working in school environments, which makes them a good target for phishing attacks. [37]

Hardening the public school services does help lower the chances of that malicious event success, but they do not cover all possible attack vectors according to "Social Engineering Attacks: A Survey" research paper [38]. The primary way to fight against social engineering attacks is to increase user's cybersecurity awareness. The computer program can detect such attacks but cannot prevent them, according to Martin Libicki [38]. Social engineering attacks involve connecting with the targeted individuals to manipulate their psychology and emotions [39].

A malware spread attack is a malicious code attack that tricks users into executing malicious programs on their local machines. Those attacks aim to paralyze, modify, or extract computer data or network systems [40, 41]. As stated in "Dynamic Malware Analysis of Phishing Emails" currently, malicious code or malware spread is one of the biggest threats on the Internet today. The issue of malware spread prevails in phishing email attacks used by teachers daily, which means that this issue persists in any other communicational

[1]Cyberphish `https://cyberphish.vuknf.lt/`

channel, for example, chat systems within the school environment. Such malware can be inserted in the attached executable files, PDF, or any other document, which makes the school environment a great target as all these types of files are distributed between teachers and students. Central defense against malware is a great filtration mechanism of an education system that does not allow users to go to unknown websites, such as phishing websites or other malicious URLs. Malware spread intends to interrupt computer operations or gain access to personal information. [41]

Another threat that can happen in a school environment is a "student as a threat". Protection from student attacks is essential as they are one of the key parts of the education process. By examining their motivation and means, it would be possible to protect teachers from students.

Cyberbullying and cyberaggression are mostly talked about in the context of student-to-student relationships. Often not only students are the targets of such aggressive methods, but teachers themselves. Mostly, cyberaggression targeting teachers is initiated by student parents or students according to "How Are Teachers Being Attacked Online? On Cyberbullying and Cyberaggression That Targets School Educators from the Student's Perspective" [42]. Such behavior can lead to a significant decrease in motivation and moral disengagement. Providing teachers with information about digital well-being is essential to increase their productivity [42]. In this article, such cyber aggression types were selected as the primary ones that are related to this thesis work:

- Disinformation on the Internet forum
- Direct attack through social media
- Video/audio recording of the teacher
- Photomontage
- Memes
- Blackmail
- Fake profiles

Another problem that every lecturer faces within the school environment is password management. The password management section would discuss efficient ways to store, use, and strategies to remember passwords to be safe.

The study "Using and Managing Multiple Passwords: A Week to a View" shows that none of the survey participants use password management tools while having high daily password usage. This article shows that even having multiple complex passwords does not lead people to use password managers. Password management tools can ease the

problems of dealing with various services without using the same password. Using a password manager is one option that teachers can use to deal with password problems. Other strategies that were also used by Grawemeyer et al. participants were offloading passwords (i.e., writing them down on paper) or sharing them with third-party subjects. Those strategies can be beneficial within the school environment to avoid losing a password. During this study, researchers concluded that during seven 7-day periods, 48 failures to enter the correct credentials happened. Password managers can prevent this issue from occurring. This study also reports that unique passwords lead to failure logins if a person tries to remember them by heart. From the discussion section, it can be learned that there are three reasons for poor password security from a user perspective: a lack of knowledge about security, erroneous knowledge, and poor strategies for coping with password overload. It is indicated that education stakeholders need to address those problems to avoid these future mistakes. The article also suggests that security policies within organizations would imply a theoretical understanding of user tasks and different psychological processes for using passwords. [43]

The guide named "Quick Guide: Cyber Security for Schools"[2] produced by NCSC (National Cyber Security Center) provides guidance for schools for password usage, which contains the following advice:

- Make use of strong and unique passwords for different services
- Use a password manager
- Create a password policy
- Limit user privileges as well as monitor their activities

[2]To be found at `https://ncsc.gov.ie/pdfs/NCSC_Quick_Guide_Schools.pdf`

3. Methodology

This section explains the methodology for learning material and both pre- and post-training survey design. Within that section, tool choice will be discussed as to why such methods fit better than others to get data for the synthesis part of this thesis.

3.1 Pre-Training Survey

The pre-training survey will employ a mixed-methods approach to comprehensively assess the current cybersecurity awareness, needs, and preferences of school educators in Ida-Virumaa. This methodology combined both quantitative and qualitative data collection techniques to ensure a nuanced understanding of the target audience's challenges and expectations.

Google Forms tools[1] will be chosen to conduct the survey. This tool was selected by the following criteria: free-to-use, anonymous data-gathering support, and multi-level questionnaire support. One more key reason this tool was chosen is familiarity for teachers inside Ida-Virumaa, as many teachers use and recommend this tool inside schools. Google Forms tool also integrates with Google Sheets[2], which will help analyze and gather data even deeper.

It is essential to design this survey in such a way that it would assert the current cybersecurity awareness of school teachers of Ida-Virumaa. Due to the language specifics of that region, this survey will be done in Russian, as future learning material will also be done using this language. Conducting a study is vital to establishing a level of cybersecurity skill and knowledge, as current cybersecurity awareness measurements were not found anywhere online during the writing of this thesis. The survey will also contain questions regarding the preference for language in future training material, as Estonia is transitioning teachers into an Estonian-only language education system. Thus, teachers can already prefer cybersecurity education in the Estonian language. To increase educator's involvement, they would also be asked about previous cyber incidents within their schools. This information would help me understand and create scenarios inside learning material that would be more real-life.

[1]Google Forms `https://www.google.com/forms/about/`
[2]Google Sheets `https://workspace.google.com/products/sheets/`

The URL of the pre-training survey in Russian can be found here: https://forms.gle/75VMMivJ7oe3wEd28. Participants' personal data, such as email addresses, was omitted to ensure privacy.

3.2 Learning Material

Developing cybersecurity learning material for school educators in Ida-Virumaa will follow the Successive Approximation Model (SAM) [6], an iterative design approach emphasizing continuous feedback and refinement. This methodology ensures that the final learning materials will be practical, engaging, and tailored to the target audience's needs.

SAM is a model mainly compared to ADDIE as an agile to waterfall model in software development. This model allows faster yet closer to the stakeholder approach, which involves iteration design and development working closely with the target audience. Compared to ADDIE this method involves multiple iteration levels over one phase with several target audience contacts for agility and better results. [6]

3.2.1 Preparation Phase

According to SAM [6] processes presented in Figure 1, the development process begins with a comprehensive preparation phase focused on understanding the educator's needs. A pre-training survey will be conducted to gather insights into the cybersecurity topics of most interest to teachers and the challenges they face within their school environments. The survey includes questions about previous cybersecurity incidents experienced in schools, such as phishing attempts or data breaches, to identify real-life scenarios that could be used within learning material. Participants will also share their preferred study methods and wishes for future training material. Some educators will be chosen to facilitate feedback systems during the iterative design process. This data will act as a foundation to guide content prioritization, ensuring that the most relevant and pressing topics for Ida-Virumaa educators will be included.

Simultaneously, a distribution platform will be selected. The primary criteria for platform selection included accessibility and ease of use, focusing on ensuring that the teachers could access the materials without registration or authorization barriers. The "sisuloomine"[3] platform met these requirements while providing robust support for H5P[4] content creation. This platform's alignment with the Estonian educational ecosystem and its familiarity with educators further supported its selection as an ideal medium for distributing training

[3]Sisuloomine https://sisuloome.e-koolikott.ee/
[4]H5P Framework https://h5p.org/

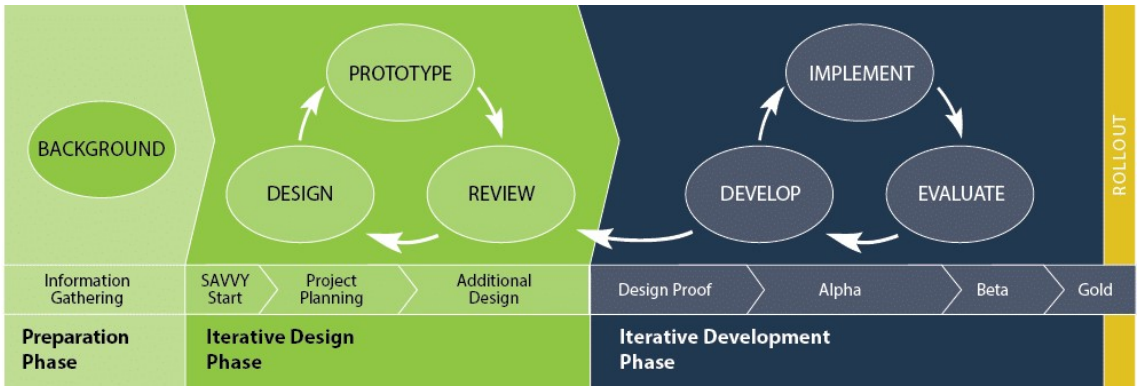


Figure 1. *The successive approximations model. Source: Allen and Sites (2012) [6]*

materials. This resource is open to everyone who would like to publish. This function can be accessed by logging in using the HarID system, which is accessible by using SmartID, identity card, or MobileID. Once the user logs into the system, it is possible to create learning material straight from the website. By default, this website provides an H5P hub for interactive teaching elements.

H5P is a free and open-source collaboration framework based on JavaScript. One of this tool's strong points is that it allows the reuse of available H5P content, if needed, by pressing the "reuse" button on the left bottom corner of any material if an author does not prohibit this function. This function fosters ideas and design sharing between creators. By providing this feature, they would not start from scratch if somebody wants to create the same learning material already available. This feature is important for this thesis work as many authors mentioned the need for knowledge transfer from educators to students during the literature review.

There are also alternatives for developing H5P content outside the "Sisuloomine" website. One option is to create interactive material within content management systems for website creation, such as WordPress or Drupal. Creating H5P materials with React Framework written in JavaScript is also possible. Both these options require local or remote server configuration. The H5P framework is also integrated with learning management systems like Moodle, Canvas, Blackboard, and others. Another option would be to create H5P material by using "Lumi H5P Desktop Editor"[5] which is available freely and can be used within majority popular personal computer operation systems today. One key feature of the H5P framework that was chosen to implement this learning material is the "interactive book" presented in Figure 2, which the Lumi editor supports. Using a desktop editor enables the editing of H5P material offline but has a significant downside. The downside is that it only supports partial interactive functionality. Only interactive supported features of

[5]Lumi H5P Desktop Editor `https://lumi.education/en/lumi-h5p-offline-desktop-editor/`

the “interactive book” content type of the H5P framework are single choice set and drag the words. After reviewing the H5P framework functionality, it was confirmed that those features are enough to provide rich and engaging learning material. This decision was made to ease the use of this material for educators, as it was not planned to be longer than one hour. Introducing too many different interactive elements could increase difficulty with the learning path of those interactive elements; rather, it would be better to concentrate on material engagement.

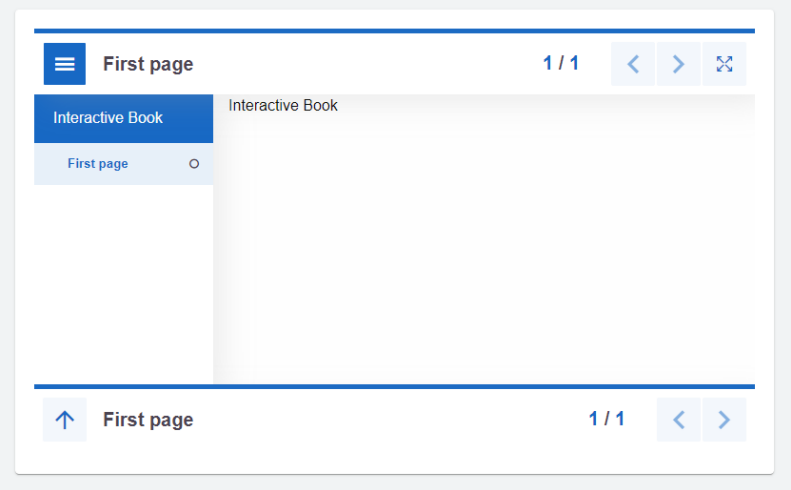


Figure 2. *Interactive book H5P element*

3.2.2 Iterative Design and Development

After the preparation phase comes the iterative design phase which involves creating and refining the learning materials through rapid prototyping. Initial prototypes incorporated gamification and interactive learning to enhance engagement and contextualize the material in real-world scenarios. Topics such as phishing, malware prevention, password protection, and personal data security will be presented through interactive challenges and basic simulations, allowing educators to apply their knowledge practically. Recognizing the linguistic demographics of Ida-Virumaa, the materials will be developed in Russian to ensure accessibility and comprehension. Gamification elements such as score system, characters, and scenario-based learning will ensure engagement and achieve better learning outcomes. These prototypes will be shared with a focus group of educators, whose feedback on usability, relevance, and interactivity will be asserted, and iteration on design will be made. This continuous improvement ensured that the materials would be both practical and user-friendly, as this thesis aimed to improve school educators’ awareness and readiness for cybersecurity challenges.

In the final phase, the learning materials will be implemented and evaluated. They will be

made publicly available on “sisuloome.e-ope.ee”, ensuring unrestricted access for all school educators in the region. A post-training survey will assess the material’s effectiveness in improving cybersecurity awareness and skills. Provided educator feedback on their engagement with the gamified elements and will offer suggestions for further refinement. The feedback loop not only validates the effectiveness of the materials but also provides insights for future development.

Through this iterative approach, the SAM [6] model facilitated the development of comprehensive and impactful cybersecurity learning material. Integrating user feedback at every stage ensures that the materials will align with the needs and preferences of Ida-Virumaa educators, ultimately contributing to their readiness to address cybersecurity challenges in their schools.

3.3 Post-Training Survey

After completing training, the target group will be presented with a post-training survey, which should be a mixed-methods approach to measure how practical and engaging the learning material was. This section should also contain information regarding the questions and tools chosen to present it more effectively to the target group.

The tools selected for this survey will involve the same toolset as those used in the pre-training study, as this will be familiar to teachers who previously filled out pre-training assessments. This decision will increase the chance of getting feedback after training completion.

This survey will focus more on the results and effectiveness of the learning material presented. All topics contained within the learning material will be presented with multiple questions to assert the level of training comprehension and memorization of the material. Another point of this survey is to ask qualitatively how teachers feel about this material and what changes they would like to see.

The URL of the post-training survey in Russian can be found here: `https://forms.gle/uok5BLJ2zKu8rTem8`.

4. Pre-Training Survey Results

In this section, the pre-training survey results will be asserted and discussed in the context of implementing future learning material for school teachers. This information would be relevant and up to date in combination with a literature review of cybersecurity threats for teachers previously done in Section 2.1.

Survey data were collected within 28.08.2024-13.11.2024 period. During that time, this list of Ida-Virumaa schools was contacted by email or the author's personal relationships. The author has chosen the three biggest cities (Narva, Jõhvi, Sillamäe) to gather information from the Ida-Virumaa region and ask teachers to complete a survey created using the Google Forms tool. The list of schools contacted is as follows:

- Narva Keeltelütseum
- Narva Kesklinna Kool
- Narva Kreenholmi Kool
- Narva Paju Kool
- Narva Pähklimäe Kool
- Narva 6. Kool
- Narva Eesti Põhikool
- Narva Vanalinna Põhikool
- Narva Eesti Gümnaasium
- Narva Gümnaasium
- Narva Täiskasvanute Kool
- Narva Õigeusu Gümnaasium
- Sillamäe Gümnaasium
- Jõhvi Põhikool
- Jõhvi Gümnaasium
- Jõhvi Kesklinna Kool

The survey data collected contains 42 answers to essential questions. From this data, we can see that the profile of survey participants is that the majority of them are females 34 (81%) and 8 males (19%) aged 35-55 years old. Most survey participants described their level of computer literacy as "proficient user" as shown by 71.4% in Figure 3.

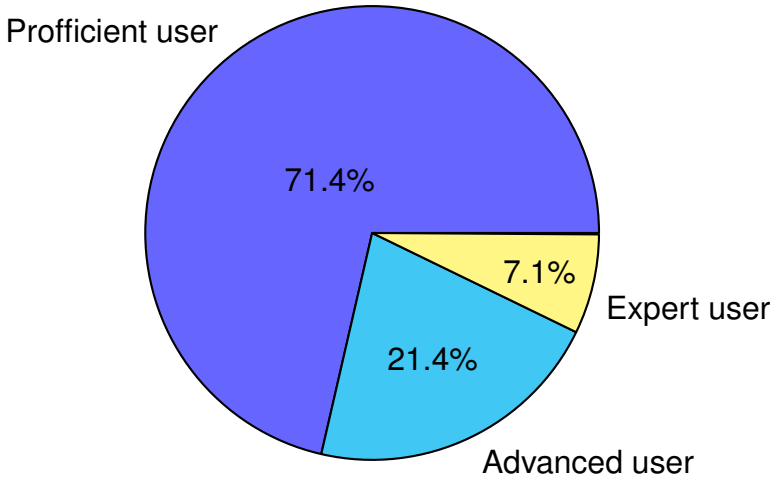


Figure 3. *How do you rate your level of personal computer proficiency?*

People who have completed a survey used many info technology tools like Kahoot, email, WordWall, and others, which is mentioned by more than 28 teachers on a 7 or more out of 10 scale presented in Figure 4. 26 out of 42 participants describe their cybersecurity knowledge level as 6-8 out of 10 scale rating shown on Figure 5. 39 participants think that cybersecurity knowledge is vital within the school environment indicating it as 7-10 on a 10 scale while having 21 answers on a 10 scale. Those one-sided reports indicate interest in cybersecurity within the school environment.

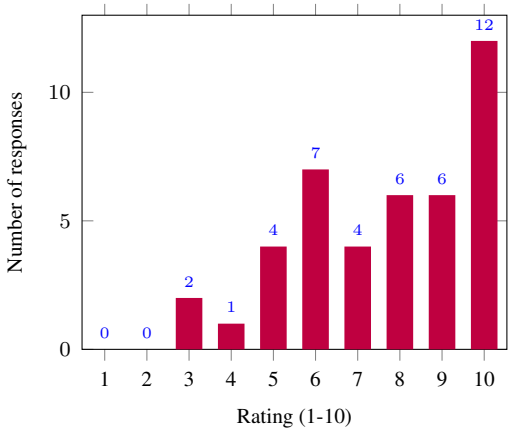


Figure 4. *How often do you use information technology in your teaching methods?*

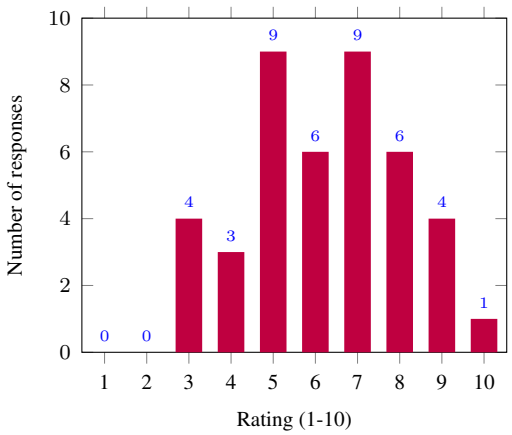


Figure 5. *How would you rate your current level of cybersecurity awareness?*

4.1 Topics of Interest

For the question "What cybersecurity topics are most important for your safe computer use at school?" the teacher's indications are presented by their relevance in Figure 6. That figure shows that personal information protection is a priority, as most teachers want to keep their personal information private from the school or class. Other topics seem to have the same necessity, including malware, secure mail handling, password security, and

secure web browsing. Also, 20 out of 42 responses indicated that “threats from students” are an issue for them. The only topic that got almost no interest at all is cyberbullying.

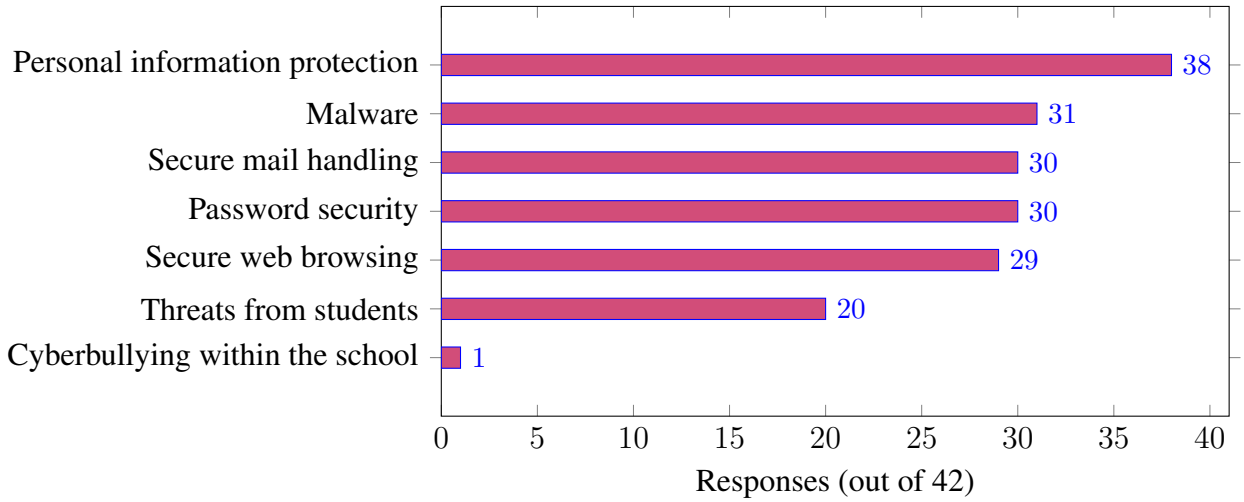


Figure 6. *What cybersecurity topics are most important for your safe computer use at school?*

To decide which topics are most interesting for teachers such questions were asked, “which cybersecurity topics would you like to learn more about to improve your readiness/awareness at school?” to which the majority answered with: “general list of possible threats”, “secure web browsing”, “malware prevention” and “personal information protection”. Next to those categories comes “password security”, “student threats” and “secure email usage”. Data for cybersecurity topics needed can be viewed in Figure 7.

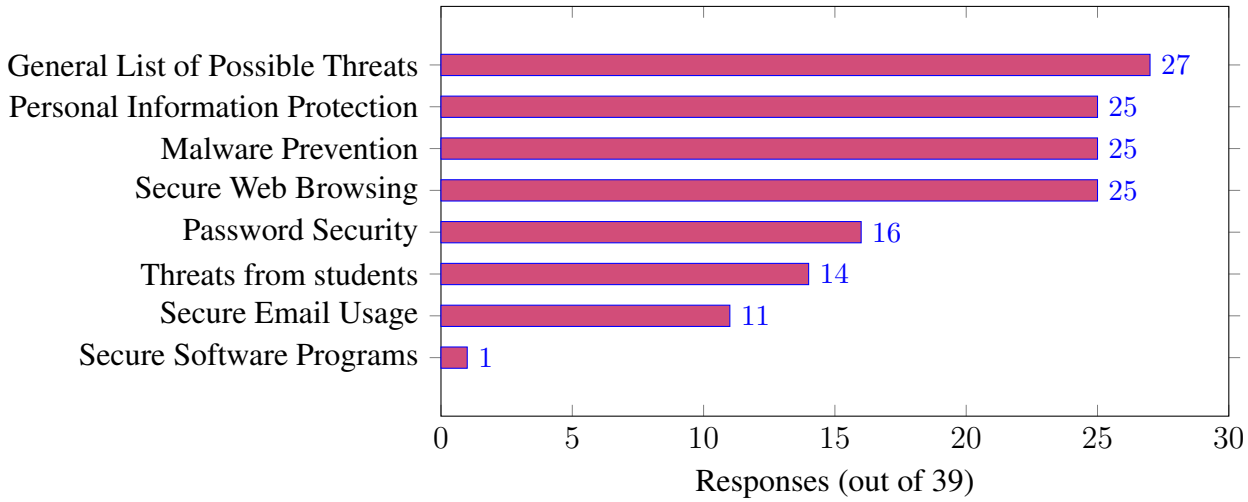


Figure 7. *Which cybersecurity topics would you like to learn more about to improve your readiness/awareness at school?*

It is also important to understand why those particular topics interest school teachers in Ida-Virumaa. From 20 answers to the survey, it is summarized as:

- Needed for everyday work
- Threat of data loss
- To be on the safe side or increase the perceived sense of safety
- That those topics are real

4.2 Cyber Incidents Inside School

The majority, 69%, never had any cybersecurity incidents within the school environment, while 31% did have some. Those incidents are summarised in this list:

- Failure to comply with inner cybersecurity rules
- Spam messages
- Virus through file sharing
- Threat messages from students, bullying
- Credentials theft
- Email confidentiality breach
- Phishing, fake emails

When asked how the school administration reacted to those cyber incidents, most survey participants answered by having meetings after an incident or doing an investigation within the school.

4.3 Previous Cybersecurity Training Experience

Most of the participants have never had any formal cybersecurity training, which is indicated by 61.9%. Those who have completed formal training previously have indicated ways of learning as such:

- Formal courses within the university
- Lessons by info technology teacher within the school
- Cybersecurity conferences
- Workplace cybersecurity education
- Web-police training
- Online courses

Most people who asked this question answered that they had studied cybersecurity at university or in school. As for the effectiveness of this training, all participants indicated 5 or more out of 10 effectiveness, as shown in Figure 8. Following that question, it was asked,

"did the training take place in your native language?" 11 out of 16 (68.8%) answered that it was not. After the native language question, it was asked, "on a scale of 1 to 10, how much more effectively would you learn the material if it were taught in your native language?" for which the majority (8 out of 10) answered that they would prefer to get cybersecurity training in their native language. This data is presented in Figure 9.

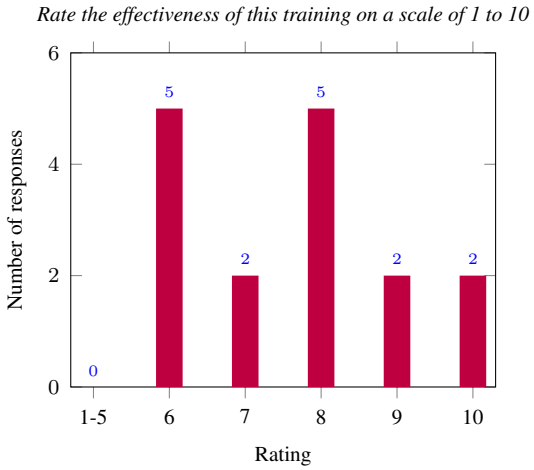


Figure 8. *Effectiveness of the received previous training*

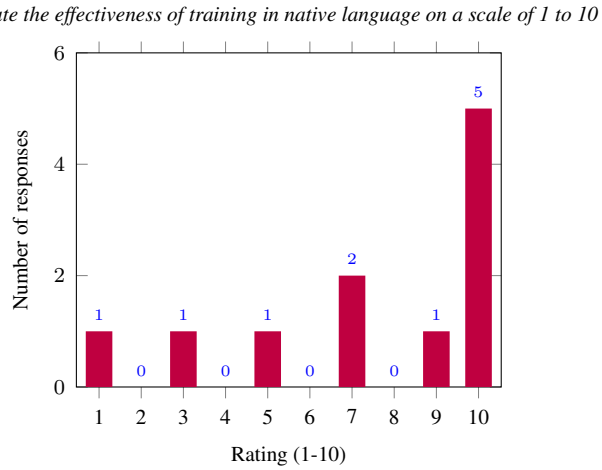


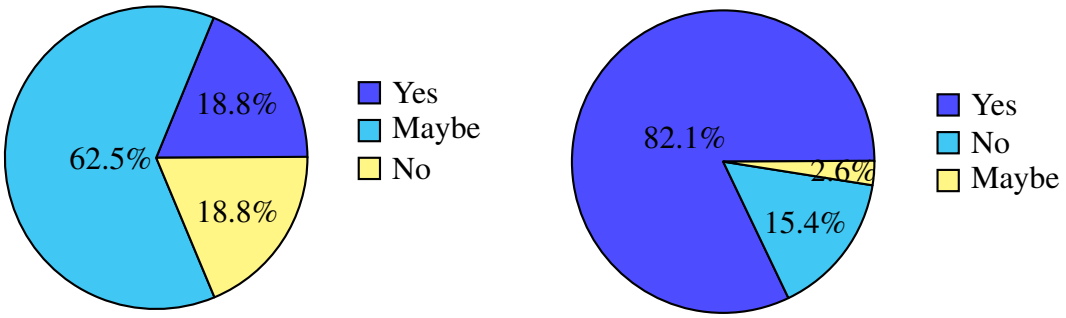
Figure 9. *Effectiveness if the training was conducted in the native language*

4.4 Methods to Improve Education Process

The next section of the survey is dedicated to methods of learning material to improve the learning process effectiveness. Participants indicated that such methods are essential: interactive platforms to test their knowledge after training, practical examples and exercises, and interactive education methods. When asked, "would you like to receive additional training to improve your cybersecurity?" 62.5% of participants chosen to answer this question answered "maybe" and 18.8% with "yes" and "no" as an answer. Those results can be seen in Figure 10. This information shows interest in improving cybersecurity knowledge and skills using interactive tools.

After answering the initial question of whether they wished to receive any additional cybersecurity education, the question was asked, "would you like to receive cybersecurity training inside the school when it is ready?" 39 participants answered, with the majority of people saying "yes" (82.1%).

Language preference is an important part of this study, as Estonia is transitioning to an Estonian language-only education system. Thus, "In which language would you prefer to receive training?" was asked. Lecturers were presented with the following options to answer this question: Russian, English, Estonian, and any. Most participants (33 out of



(a) *Would you like to receive additional training to improve your cybersecurity skills?*

(b) *Would you like to receive cybersecurity training inside the school when it is ready?*

Figure 10. *Interest in receiving additional training in cybersecurity*

39) prefer "Russian" (85%) as the language for training instructions. 8 out of 39 (21%) participants would like to study in Estonian, while only 5 (13%) lecturers prefer English. Only 3 personas state that they would be ready to train in any language out of Russian, Estonian, and English. This information highlights a need to develop training in the Russian language as most people requested to get content in that language. Providing content in the native language of participants, which is 40 out of 42, would also increase accessibility and engagement, fostering more understandable and insightful content. This data can be viewed in Figure 11.

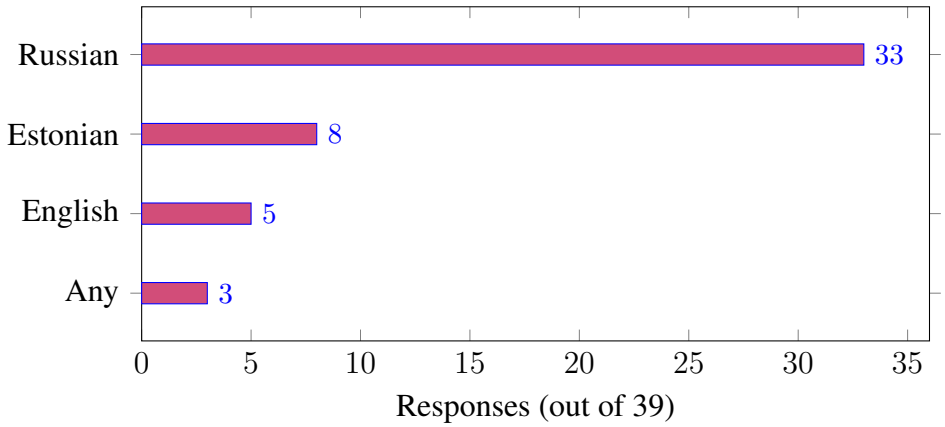


Figure 11. *In which language would you prefer to receive training?*

4.5 Summary of Pre-Training Survey

The survey provides insights into Ida-Virumaa teachers' cybersecurity knowledge, training preferences, and perceived needs for enhanced cybersecurity awareness, especially within the school environment. Here is a summary of the findings:

1. Preferred study material and training:
   - Teachers expressed interest in interactive, practical cybersecurity education,

including platforms for self-testing, exercises, and engaging teaching methods
    - When asked about receiving additional training, 62.5% answered “maybe”, while only 18.8% choose “yes” or “no”
2. Cybersecurity topics of interest:
    - The most requested topics were general cybersecurity threats, secure web browsing, malware prevention, and personal information protection
    - Secondary topics of interest included password security, handling student-related threats, and secure email practices
    - Teachers highlighted these topics as relevant due to daily work needs, data security concerns, and a desire for greater safety
3. Language preference for training:
    - The majority (85%) preferred training in Russian, emphasizing a need for Russian-language resources to increase accessibility and comprehension
    - A smaller number preferred Estonian (8 participants, (21%)) or English (5 participants, (13%)).
    - Offering content in participants’ native language (Russian for 40 out of 42) would improve accessibility and engagement.
4. Demographics and digital proficiency:
    - The participants were primarily female (80%) aged 35-55, with a high level of computer literacy; 70% identified as proficient users
    - Teachers used a variety of digital tools regularly (e.g., Kahoot, email, Word-Wall), and 61.9% rated their cybersecurity knowledge at 6-8 out of 10
5. Cybersecurity relevance and incidents:
    - 21 out of 42 teachers viewed cybersecurity as essential in schools. Key areas of concern included personal information protection (38 responses), malware, secure email, password security, and safe web browsing
    - Although 69% reported no direct cybersecurity incidents at school, 31% had encountered issues such as phishing, virus infections, spam, and breaches of email confidentiality
    - Schools typically responded to incidents by conducting internal meetings and investigations
6. Training experience and language barriers:
    - Most participants (62%) had no formal cybersecurity training. Among those who had, the training came from diverse sources, including university courses, school IT lessons, cybersecurity conferences, workplace training, and online courses
    - A significant portion did not receive training in their native language. When asked about the effectiveness of native language instruction, the majority indicated they would benefit more if cybersecurity training were offered in

their native language

7. Effectiveness of training:
    - Those who had undergone training rated its effectiveness as 6 or above out of 10, reflecting a moderate but promising impact
    - 6 out of 11 participants who have undergone cybersecurity training not in their native language believe they would receive more efficient training if it were in their native language

The survey findings suggest that while cybersecurity awareness is valued, there is a strong need for accessible, practical, and language-tailored training resources for school teachers in Ida-Virumaa, particularly in Russian. Enhanced educational materials could better equip teachers to handle digital threats in schools.

The URL of the pre-training survey data in Russian can be found here: `https://docs.google.com/spreadsheets/d/1nklm2RWwkAzWP7AXwj7ed3grZnIar8QA7kGfv7E4Ox0/edit?usp=sharing`.

5. Learning Material Development

To create effective learning materials for educators in Ida-Virumaa, it's essential to use a variety of techniques that boost engagement and provide teachers with compelling reasons to use this tool. Since many teachers are new to cybersecurity training, as indicated by pre-survey responses, incorporating storytelling and gamification strategies can help spark interest and enhance learning on this topic. Fariza Khalid and Tewfiq El-Maliki [44] describe digital storytelling as a powerful tool to improve engagement in the learning process. To create an engaging story for educators, it is essential to canvas stories for learning material. The story can be produced by using a combination of visuals, photos, drawings, voice narration, and music [44]. Using storytelling could simplify complex topic understanding for end-user learners, according to "Digital Tools, Approaches and Assessment for Cybersecurity Education via Storytelling: a Systematic Literature Review" article [45]. The story of these learning materials plays a key role in engaging and interesting educators as they are strict on time and unfamiliar with the cybersecurity field. By providing a close-to-heart tale, it would be possible to show teachers how to connect cybersecurity and their daily education routine.

The story's main line is based on the person getting inside a cyber-oriented school as a regular teaching staff member, who is cyber-attacked by different students daily. This scenario fosters an opportunity that can happen in real life due to varying levels of computer literacy between schools in other countries or cities. After getting inside the teacher role in front of the teacher comes five days of challenges, presenting a typical working week. Each day of this adventure, the educator will be presented with a different topic in cybersecurity and the related fictional person who tried to breach him in various ways. The first-hand teacher meets with a day's introduction, after which comes the challenges. The challenges are led by information related to the task itself; for example, if the topic is malware, it is followed by details regarding different malware types. After the challenges provided information block explains the topic more deeply, providing information and behavior patterns to avoid such cyberattacks. Each day concludes with day-end text to conclude what this day covered and why it is essential to understand this topic. To create an experience closer to life, a persona with widely-used names represents a threat as a person and creates more gamified content. The summary of study days can be viewed in Table 1.

Table 1. *Learning material summary*

Nr	Name	Summary
1	Greetings	Introduction information and one single-choice set question.
2	Day 1: Phishing From Alina	An attack through email with a phishing link. This day also contains three single-choice set questions and two definitions.
3	Day 2: Malware From Petya	Malware spread attack. During this day, malware types and definitions were discussed. The day ends with a drag-the-words challenge.
4	Day 3: Personal Data From Sveta	Personal information gathering through the messager app. Followed by a drag-the-words challenge to assert which information should stay private. Afterward, information blocks explain why the confidentiality of personal information is important.
5	Day 4: Device Protection From Kirill	Contain challenge to set the best privacy settings for mobile device applications. Followed by an explanation of why certain settings are important to turn off.
6	Day 5: Brute-Force From Maksim	Password-protected .zip brute-force prevention challenge. Followed by information about brute-force and password leaks.
7	Wrap-Up	Contain multiple tests on key characters and their aim during the cyber week and overhaul drag-the-words challenge for definitions. After the training concluded, educators were asked to fill out the post-training survey.
8	Additional Materials	Contain links for cybersecurity learning material found during this thesis work.
9	Library of Definitions	This page contains all definitions from training material in one place for easier search for educators.

5.1 Each Day in Details

"Greetings" is the first day inside this learning material, which contains introductory information about the exercise. This information is necessary to establish a clear and visible goal to archive for educators of Ida-Virumaa. This material aims to enter "CyberSchool"

as a new teacher, with the knowledge that all students of this class will be cyber-aggressive and computer literate. Following that introductory information, a simple question is asked, "are you ready to become a CyberTeacher?" which is created to make sure that the person attending education material has read the introductory material well and is ready for the challenges ahead.

Phishing attacks are one of the most widespread types of attacks in cybersecurity. That is why "monday" in cyber school is "day 1: Phishing from Alina". During this day, Alina, a fictional character in a cyber class, will try to gather school credentials from her teacher by conducting a phishing attack through email. She sends a phishing link from her mother's address through an email to promote the urgency and the importance of taking action. This email contains visible mistakes that the teacher can recognize and act accordingly. At the end of the single-choice question set, the teacher asked about strategies for dealing with that in real life, step by step. After the interactive material comes two information pieces: "what is phishing?" and "what is 2 factor authentication (2FA)?". The phishing part explains what phishing is and how to recognize it within websites and emails. The 2FA information must familiarize the teacher with the definition and how it works. This part also contains examples of using 2FA and why it is essential to be set up if available. Those two information blocks are necessary to explain to the teacher how to protect himself from possible phishing attacks in the future. After those blocks, a summary of the day follows. This block concludes with information about why Alina wanted to do that and which people's property she tried to abuse to get teacher credentials.

"Day 2: malware from Petya" starts with presenting a fictional person, Petya, who tries to upload some malware to the teacher's work computer. Afterward, an analysis of one malware file contained in a password-protected .zip archive was presented to recreate a real-world scenario, sending malware within a password-protected archive is currently possible using email. The introductory block is followed by a single-choice answer test about malware presence within this file and malware type, which is visible in VirusTotal[1] output presented as a picture. A link to the website, represented by a picture, is also provided. The challenge set concludes with a possible plan to deal with this situation in real life. After comes the information block, which contains definitions of malware and malware types. The author has chosen only four types of malware to make it easier for educators to grasp the topic while still going deeper to gather interest. Those information blocks contain all the necessary questions on how to protect, why a particular type is dangerous, and how it works. The next block is the drag-the-words challenge of type of malware definitions, as the information block of day two was bigger in size than the usual information block of this learning material. This challenge is also essential to gaining

[1]VirusTotal `https://www.virustotal.com/`

learner's interest in reading more about malware types. This day concludes with the day's finish message, congratulating the user on their progress and inviting them to go the next day. Day 2 challenge is essential to motivating educators to use virus scanning tools on suspicious files before executing them in their day-to-day school activity.

In "day 3: personal data from Sveta" the personal information protection topic is presented in gamified form introducing the fictional person Sveta. She would like to gather personal data to recover the passwords of educators by asking them to fill out the questionnaire as a new teacher in class. Sveta asks that through group class chat, a safe channel to answer any questions inside the school. The questionnaire is presented to the teacher, and they need to decide which questions are suspicious and which are secure. Afterward, provided information regarding the safety of personal data usage and how that data can be used against the educator. Next, the information block explains why the confidentiality of information is essential and how to act if some information leaks into the public. As in previous days, day 3 also concludes with the conclusion of the day and asks to move to day 4. Personal information protection was one of the topics that were highly requested to be covered. Day 3 material does not cover this topic from every possible corner, but it provides valuable lessons that any information, even the pet's name, can be used against the educator. This lesson's main aim is to ensure that the teacher thinks about how personal information can be used against him before spreading it over the internet or in person.

Mobile phones are used daily in our lives, as well as in work conditions. That is why "day 4: device protection from Kirill" is a vital topic for the educator group to cover. Usage of applications raises significant over websites on mobile in 2025[2]. Due to that fictional person, Kirill tries to gather mobile phone data through his self-made application, which should help the teacher in his day-to-day process. This lesson focuses on providing valuable information regarding mobile application privacy settings. This day starts with introducing Kirill's application as a helpful tool in the teacher toolset, followed by screenshots of multiple "asks for permission" messages. Those messages present an artificial intelligence chatbot, asking way over what is needed to function as a chatbot. Afterward, a one-choice answer test will be shown to establish that so many permissions are not required for his application to function. Next comes the drag-the-words challenge to restrict Kirill's application to the maximum to prevent unnecessary data access. After challenges presented an information block on why restricted functionality access is essential and how the threat actor can collect various data, such as photos, contacts, geo position, etc. This block also contains information regarding the restriction level of particular functionality and how it can be decided. Afterward comes the end of the day, which concludes why Kirill should

[2]Mobile Apps vs Mobile Websites (Why 90% of Mobile Time is Spent in Apps) `https://www.mobiloud.com/blog/mobile-apps-vs-mobile-websites`

not get too much data from teachers' phones and invites them to follow up the next day. Setting restrictions to prevent private information leakage inside your phone is essential for educators, as uneducated users could not know what particular "yes" inside their mobile application settings means. This knowledge would help educators restrict unnecessary access to phone data and/or functionality.

"Day 5: brute-force from Maksim" starts with an attack scenario from fictional student Maksim. The teacher presented with a flawed way of saving their credentials in a password-protected .zip archive. Maksim sees this opportunity to gather teacher data, and once the teacher leaves his classroom, he steals this .zip archive to brute-force it at home. Next presented is a single-choice answer test, which shows that some passwords could be guessed by brute-force attack in 10 seconds. Afterward comes an information block on what brute force is and how it works. Also, this block contains information on why, in some programs (for example, .zip archive), it is easier to guess the password. Next comes information regarding password manager usage and why it is a better option for password safety. This block concludes with an explanation about data leaks and how to check your email address through "Have I Been Pwned"[3] service. The day finishes with a conclusion about brute-force usage and how to make it more difficult to guess your password. This topic is essential for educators as they have multiple credentials for different services inside their schools. Providing real-world examples of why setting easy-to-guess passwords is not the best idea would help educators understand the importance of long and hard passwords.

"Wrap-up" day concludes training with two final tests which assert if the educator remembers each attacker by name and is familiar with definitions that are presented during material. Next, the remaining pages are presented, including "additional materials" and a "library of definitions". This page also invites educators to reuse the content of this training material if needed and asks them to fill out a post-training survey. "additional material" links include website links found during this thesis writing and contain a YouTube video, an NCSC-EE YouTube channel, an article, and the "targalt internetis" website. The "library of definitions" combines all definitions found through learning material and presents them in one place for easier search and accessibility. These elements would benefit the engagement and usability of this learning material for educators of Ida-Virumaa.

5.2 Iterative Design and Development

As mentioned in this thesis's methodology section 3.2, the SAM framework [6] requires close work with the target audience. Five persons were chosen to gather feedback during

[3]Have I Been Pwned `https://haveibeenpwned.com/`

the rapid development of this training material to make the best out of this requirement. Most design elements were selected from real-world systems, like iPhone interface, Gmail, or websites. Thus, the iterative design phase does not require more than one iteration to gather the needed results to go straight to the development phase.

During the iterative development phase, most of this material was created during the "design proof" [6] phase, which ended up in a current version of the training material distributed between educators of Ida-Virumaa. During this iterative development phase, key suggestions were to add more graphics, explain what malware is, change some definitions translations, add a library of definitions, and correct some mistakes.

According to SAM [6], the next development phase is the "alpha" phase. One of the author's concerns was that training would take too much time to accomplish, as some participants indicated they were short on time during pre-training data collection. As this was one of the concerns, each participant was asked during the "alpha" phase if this training was not too long for them and if they could complete it within 1-2 hours of learning. Only one of the participants indicated that training can be too long for the teachers to accomplish. Others suggest that this is well enough for reasonable training and a great introduction to the cybersecurity field for educators of Ida-Virumaa. Another improvement made during the "alpha" phase was rephrasing literature aphorisms, which could be rephrased for the text to be more precise.

The next development iteration, according to SAM [6] of learning material, is the "beta" phase with a bigger group of Ida-Virumaa teachers, which will be evaluated during post-training survey research. The "beta" phase will be last during the current thesis work as the "gold" phase should be implemented after receiving more feedback data from teachers than planned gathered in the post-training survey.

The URL for the final results can be seen here: `https://e-koolikott.ee/ru/oppematerjal/34497--1-12`.

6. Results

The interactive learning material created within that thesis work demonstrated a significant impact on cybersecurity awareness among school teacher groups. The completion rate of 8 out of 30 successfully finished educators suggests high engagement and satisfaction, with participants reporting improved knowledge and skills to manage inner school environment tools more safely. Unfortunately for some reason unknown to author 2 responders did not provide their agreement to work with their data. Due to the anonymous survey study, it is impossible to assert why they made that decision nor was it done by mistake or not.

Post-training surveys started with an assessment of previous levels of knowledge in cybersecurity. 50% of participants declare that they have a confident level of cybersecurity knowledge, 33.4% advanced level, and 16.7% novice. This information shows that the majority of training participants were previously experienced in the cybersecurity field. A confident and advanced level of cybersecurity awareness can help understand the current status of the material and how helpful it will be for other school teachers.

100% of the teachers who completed training stated that their interest in the cybersecurity field increased. When asked how much material helps improve their cybersecurity knowledge on a scale from 1 to 10, 2 educators stated that it is a 10, 2 teachers suggested a rating of 8, and 1 for each 6 and 7 categories. Such great results indicate that this material can be seen as a great tool to increase cybersecurity awareness and knowledge even for mostly advanced teachers.

Of the 6 topics of this training material for 83.3% educators, the most new topic is “malware prevention”, which is understandable as most operating systems protect from such threats. The next category is “phishing” indicated by 66.6%, which is alarming information as this type of attack is mostly spread. Teachers working daily with email and unfortunately can become a target for attack using this channel. Afterward comes “personal data protection”, and “device information security” indicated by 50% of participants as a new topic for them. “password security” topic was indicated as a new topic by only 33.3% of educators. Results show that all topics chosen during the pre-training survey and literature review were correctly selected as all of them were new to some portion of the training participants. Question results can be seen in Figure 12.

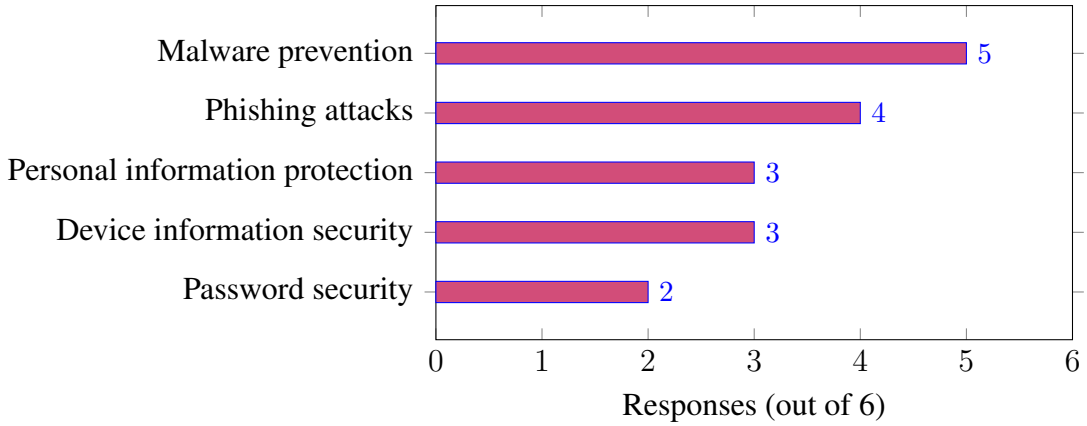


Figure 12. *What topics from the training were new to you?*

6.1 Training Material Topics Comprehension

The training material topics comprehension section will cover each section one by one to understand the weak and strong points of the material created. By asking educators particular topic questions it would be possible to assert a level of understanding and engagement.

6.1.1 Phishing Attacks

Half of the responders state that they are going to recognize phishing attacks. The other half thinks that it would be possible to recognize such an attack if some obvious properties were presented. From this information, the author can conclude that every participant is now aware of what is a phishing attack and ready to deal with this cyber threat in the future.

The following questions to ensure that they can recognize phishing attacks were asked as such: “which of the following is most likely to indicate a phishing email?”. This question contained such options as: spelling mistakes in the text; unusual address of the sender; urgent call to action; and the presence of a link in the letter. Unfortunately, the results of these questions were split equally between all options indicated by 5 participants each. All those options can be interpreted as a correct answer, but links in an email a standard operations and do not mean that email is a phishing one. Otherwise, results indicate that educators have gone through materials and remember all the usual indicators on how to recognize a phishing email.

6.1.2 Malware Prevention

The malware section of the post-training survey asked questions to ensure that educators understood the malware topic presented in the training material. The first question was: "what would you prefer to do with a suspicious file?", the majority answered that they would scan the file for viruses first which is indicated by 66.7%. Others choose to delete files without a virus scan. 0% of participants chose to just open the file and see how it will execute. This is a great result as 5 participants indicated that the malware topic is new for them.

For the next question "what action helps minimize the risk of device infection?" 100% answered that they will "download applications and files only from trusted sources". Other options presented as answers to this question were: ignore program update messages; and open all attachments in emails to check their contents. As the majority of participants were not novice learners in cybersecurity this question was too easy to answer correctly, but the 100% right result indicates that responders understand how to protect themselves from malware attacks.

6.1.3 Personal Data Protection

To ensure that the training material of the personal data protection section is understandable and comprehensive teachers were asked a couple of questions on that topic. One multiple-option question was "what data is most vulnerable from the leaked data?". Options presented as answers were: personal photos; logins and passwords; financial information; email; name and last name. All participants think that passwords and login are the most valuable assets in leaked data as they can be used to gather more different data. The next favorite option chosen by 5 personas is financial information. Followed by equally rated "personal photo" and "name and last name" selected by 50% of training participants. The most unfavorite option was an email selected by 2 educators. Results suggest that those who finish this training material understand the meaningfulness of every presented as option personal data and can act accordingly to not spread sensitive information.

Next educators were asked on their way to secure inventory of their passwords. Options for this question were: on paper; in text document; and in a password manager. Results are split equally for 2 options which are on paper and password manager. Both methods are popular, but they highlight differing levels of awareness and trust in digital security tools.

6.1.4 Device Information Security

Device information security topic covered by asking the following question: “which application access rules are more crucial to restrict?”. Access restriction options for teachers to choose from were: camera; location; contacts; and photos. Survey participants choose to select all options as an answer. This information shows that they cannot prioritize any form of access rules from those options for themselves and choose to restrict every access possible as it was suggested in the learning material itself.

The second question for that section was: “what have you changed on your device after training?”. To answer this question such options were presented: installed antivirus; turned off unnecessary application rules; nothing. 3 out of 6 participants answered that they turned off unnecessary application rules which was the main learning point of “day 4: device protection from Kirill”. 1 participant chose to install antivirus after this learning program, which was not strictly mentioned during training material, but can be an option to lean towards after completing training. Unfortunately, 2 personas chose to answer that they have done nothing, which can suggest that they do not understand this topic or they have already experienced enough to maintain the right access rules on their device beforehand.

6.1.5 Password Security

Password security topic is one the least novel to a survey participants. As the majority of educators who have completed this training are advanced users all participants managed to answer all questions in the password security section correctly. To make sure that topic is covered and understood by teachers 2 simple one-choice questions were asked: “which password is most secure?” and “how will you check if your data have been leaked?”. All educators have successfully chosen the most secure password from 3 options: qwerty123; ilovepizza2024; and k1ber_$chola2025. This question can be viewed as too basic, but it was important to make it this way as the majority of pre-training survey participants stated that they are not familiar with cybersecurity.

Another question, which is “how will you check if your data have been leaked?” contained such options: it is impossible to check; by using special services (like haveibeenpwned.com); and by paying fees from specialists. This question was answered correctly by all survey participants and shows that they have been studying through this particular section.

Password security topics are one of the more widely spread and examined during regis-

trations on different services, so it could be too easy for average cybersecurity-educated teachers. On the other hand, as most pre-survey participants have not done any cybersecurity training before this topic was important to cover during this thesis work. Password security topic is a starting point for basic cybersecurity of teacher's data.

6.2 Overall Feedback

Feedback on the learning material received was very positive, with ratings of more than 8 out of 10. 50% of participants rated this training as 10, which is a great result and suggests that the methods used to engage and create a meaningful learning experience were chosen correctly. 83% of survey participants also indicated that the material was fully understandable and accessible, and only one person indicated a good level of understanding.

As this training used the SAM [6] model as a reference for design and development participants were asked to highlight trouble areas of this training. 2 educators highlighted that some grammar mistakes are still in the text and that some definitions translated into the Russian language are not the same in training material. 1 teacher highlighted a problem with drag-the-words challenges as it is not very intuitive how to paste answers, particularly drag functionality does work very specifically. This answer is very helpful and the author thinks that some type of explanation on how to use drag-the-words functionality should be added in the future or used some other method of gamification. The drag-the-words issue was also captured during "alpha" phase, but the author's comment on how to use it properly solved this problem with one that had it. If more data suggest that this issue persists, then a guide page should be added to this material.

The next section of the survey question was dedicated to the plans of educators after training material completion. 66.6% of participants are planning to share acquired cybersecurity knowledge and this learning material created within this thesis work with their colleagues, others indicate that they may share it. Such a high engagement suggests that learning material reaches its aim and raises interest in learning cybersecurity and sharing their knowledge with their peers.

6.3 Summary of Post-Training Survey Results

The interactive learning material developed in this thesis had a significant impact on cybersecurity awareness among school teachers. Of the 30 participants who were interested in receiving training material, 8 teachers successfully completed the training, demonstrating high engagement and satisfaction. However, 2 participants declined to provide consent for

data usage, which could not be clarified due to the anonymous nature of the survey.

1. Pre-Training Knowledge Levels
   Before the training, participants cybersecurity knowledge levels were as follows:
   - 50% — Confident level of knowledge
   - 33.4% — Advanced level
   - 16.7% — Novice level

   These results suggest that most participants had prior experience in cybersecurity, which informed their understanding and engagement with the material.
2. Post-Training Outcomes
   After completing the training:
   - 100 of participants reported increased interest in cybersecurity.
   - On a scale of 1 to 10 for how helpful the material was:
     - 2 participants rated it 10
     - 2 participants rated it 8
     - 1 participant each rated it 6 and 7

   These positive ratings indicate that the material effectively enhanced the participant's knowledge and skills.
3. New Topics Learned
   Among the six training topics, the most novel for participants were:
   (a) Malware Prevention — 83.3%
   (b) Phishing — 66.6%
   (c) Personal Data Protection and Device Information Security — 50% each
   (d) Password Security — 33.3%

   This confirms that all selected topics were relevant and valuable to the participants.
4. Training Material Topics Comprehension
   The comprehension of each training topic was assessed through specific questions:
   (a) Phishing Attacks
      - 50% of participants felt confident identifying phishing attacks
      - Responses to a question about phishing indicators were evenly split among spelling mistakes, unusual sender addresses, urgent calls to action, and links in emails — showing broad awareness of phishing signs

   (b) Malware Prevention
      - 66.6% would scan suspicious files rather than deleting them outright
      - 100% agreed that downloading from trusted sources minimizes infection risks

   (c) Personal Data Protection
      - All participants identified passwords and financial information as the most valuable data

        - Password storage methods were split between paper and password managers, reflecting varying levels of trust in digital security
    (d) Device Information Security
        - All participants prioritized restricting app access to camera, location, contacts, and photos
        - 3 participants turned off unnecessary app permissions after the training
    (e) Password Security
        - All participants correctly identified secure passwords and knew how to check for data breaches
5. Overall Feedback and Suggestions
    - 50% of participants rated the training 10/10.
    - 83% found the material fully understandable and accessible.
    - Suggestions for improvement included:
        - Fixing grammar and translation issues
        - Improving the "drag-the-words" functionality
6. Future Impact
    - 66.6% of participants plan to share gained knowledge and the material with colleagues, highlighting the training's potential for broader impact

The URL of the post-training survey data in Russian can be found here: `https://docs.google.com/spreadsheets/d/1fOlQvtQix6jo85InZIJfB1WGMQ5C1YReSxOedU9ltxw/edit?usp=sharing`.

6.4 Research Questions Answers

What are the specific features of cybersecurity training for school teachers in Ida-Virumaa (in the context of the Russian-speaking majority and lack of cybersecurity education in this language)?

The cybersecurity training developed for school teachers in Ida-Virumaa possesses several unique features that reflect both the regional and linguistic landscape of the target group. These features were informed by pre- and post-training surveys, literature analysis, and the practical needs of educators in this predominantly Russian-speaking region.

One of the most critical features of the training was its delivery in the Russian language. Pre-training survey data revealed that 85% of participants preferred training in Russian, underscoring a significant language barrier in existing cybersecurity resources. Only 21% choose Estonian as an option for language preference in training material. The developed material directly addressed this gap by offering linguistically appropriate content, which

participants rated as highly understandable (83% found this material fully accessible). The inclusion of native language content improved not only comprehension but also overall engagement and satisfaction with the training experience.

Pre-training survey results indicated that teachers were most interested in learning about general cyber threats, personal information protection, malware prevention, secure web browsing, password security and student-originated cyber threats. Some of these topics were incorporated into the training to ensure direct relevance to teachers' professional responsibilities and digital safety needs. The focus on practical, everyday issues made the training immediately applicable in the school environment. Post-training data confirmed that these topics aligned with teachers' needs. Malware prevention was perceived as the most novel topic by 83.3% of participants, followed by phishing (66.6%), personal data protection (50%), device information safety (50%), and password security (33.3%).

Another notable feature was the interactive and task-based nature of the training. Teachers had previously expressed a preference for self-testing opportunities, exercises, and practical applications of knowledge. The developed training incorporated these elements through quizzes, drag-and-drop exercises, and scenario-based questions. This design fostered active learning and deeper engagement. Teachers responded positively to this format, with 100% of post-training responders reporting an increased interest in cybersecurity. Also, 66.6% indicated plans to share gained knowledge and material itself with colleagues, suggesting both satisfaction and perceived value of the content.

What teaching methods or pedagogical approaches effectively convey cybersecurity concepts to school teachers in ida-Virumaa?

The effectiveness of cybersecurity education for school teachers in Ida-Virumaa was largely shaped by the pedagogical methods employed during the training pilot. Pre- and post-training survey responses offer direct insight into which approaches were most appreciated by participants and how they impacted learning outcomes in this specific context.

Before the training, participants indicated a preference for interactive platforms, practical examples, and exercises as the most important features for effective cybersecurity education. These preferences guided the design of the training, which focused on drag-and-drop tasks, and knowledge-check quizzes embedded throughout the modules. The participants' feedback validated these choices, with 83% stating that the material was fully understandable and accessible. Half of the participants (50%) rated the material a perfect 10 out of 10, reinforcing the value of active, experiential learning.

While the training did not involve full-scale gamification (such as competitive challenges or achievements system), it did include interactive, game-like components, such as quizzes and drag-the-word challenges. These were well-received overall, although minor usability issues were noted by a small number of participants. One teacher, for example, commented on the unintuitive interface of the drag-and-drop activity. Despite this, post-training ratings remained high, suggesting that gamified elements contributed positively to engagement and learning when they were intuitive and well-explained.

The training created during this work supports self-paced learning, allowing educators to engage with the material on their own schedule. This flexibility was a significant advantage for working teachers, as it respected their time constraints and diverse learning speeds. The asynchronous nature of the training contributed to high participation and completion rates, with 66.6% of participants expressing intent to share what they learned with colleagues, indicating that the training was not only comprehensible but also meaningful and empowering.

Survey responses before and after the training reveal that school educators in Ida-Virumaa benefit most from interactive, practical, and linguistically accessible learning methods. These preferences directly shaped the training structure, resulting in high satisfaction, strong comprehension, and a clear willingness to continue cybersecurity education. While minor technical or linguistic adjustments are still needed, the core teaching methods have proven to be highly effective in this specific regional and cultural context.

What resources (e.g., training materials, workshops, online courses) are currently available for school teachers in Ida-Virumaa?

The analysis of existing cybersecurity resources reveals that materials specifically tailored for school teachers in Russia are extremely limited. During the writing of this thesis, some materials provided by Estonia have been removed. Most resources available are either too general or not designed with educators in mind. A few notable resources include:

- Chuiko Roman's Youtube video [12] provides foundation cybersecurity knowledge in Russian, covering key topics like cyber threat vectors, 2FA, and password management. However, this material was created in 2020 and is provided by an institution in Russia.
- The article "Cybersecurity for Teachers - What Should You Know in 2025?" [13] offers practical tips for classroom management, internet safety, and student-related risks. It stands out for its applicability in schools and multi-language accessibility but is not part of a structured training program.

- The “ITVaatlik” [14] website offered short, visual, interactive resources in Russian, such as tests and guides on social media safety and phishing recognition. This website does not focus on teachers specifically but is a great interactive resource for cybersecurity learning available in the Russian language. While it was a helpful starting point, as of 2025, all Russian-language content has been removed, significantly reducing accessibility for non-Estonian speakers. This resource is still available by using “web.archive.org”[1].
- “TargaltInternetis” [15] offers useful event information and student-focused teaching resources. However, its partial Russian translation limits accessibility, and the focus remains primarily on student education rather than teacher skill development.
- The RIA YouTube channel [16] includes Russian-subtitled videos with general cybersecurity advice, accessible to beginners. Though useful, it lacks interactivity and pedagogical structure for teacher training.

While some general cybersecurity resources exist in the Russian language, there is a significant gap in structured, engaging training specifically for school teachers in Ida-Virumaa. Most resources are not tailored to educators’ needs, and with “ITVaatlik” [14] removing all Russian-language content in 2025, access to reliable materials in the region’s majority language has further diminished. This underscored the critical importance and timeliness of the training program developed in this thesis.

Which cyber threats are most dangerous and should be prioritized? What topics (e.g., safe internet practices, data privacy, threat awareness) should be emphasized?

The most dangerous cyber threats facing teachers in public schools include phishing attacks, malware spread, personal data breaches, password mismanagement, and student-initiated cyber threats. Phishing, often used as an entry point for other attacks, exploits human trust and urgency, making it a critical concern. Malware frequently accompanies phishing attempts, posing a high risk in environments where teachers regularly exchange files. Additionally, poor password habits and limited use of password management tools make school systems more vulnerable. Teachers are also at risk of cyber aggression from students, including social media attacks and disinformation.

Survey results confirm these threats align with teachers’ main concerns, highlighting strong interest in topics such as personal information protection, malware prevention, secure web browsing, password security, and secure email usage. These areas should therefore be prioritized in cybersecurity training programs. Training should emphasize human-factor

[1] https://www.itvaatlik.ee/ru/ `https://web.archive.org/web/20241005021751/https://www.itvaatlik.ee/ru/`

awareness, safe internet practices, and practical data security skills to improve digital safety in the school environment.

What level of preparedness do they currently have to address cyber threats (in the context of the Russian-speaking majority and lack of cybersecurity education in this language)? What could be done to improve preparedness?

The level of preparedness among school teachers in Ida-Virumaa to address cybersecurity threats is moderate but uneven, shaped by a combination of prior digital experience, high demand for Russian-language content, and a general lack of formal training. Current level of preparedness:

- Pre-training survey results revealed that 62% of teachers rated their cybersecurity knowledge between 6 and 8 out of 10, and 70% identified as proficient users of digital tools, suggesting a solid foundational digital literacy. However, this self-assessed proficiency often lacked a structured understanding of cyber threats.
- 69% of participants reported no formal cybersecurity training, and those who had such experience often received it through informal means such as workplace seminars or university lectures not tailored for the school context. Importantly, most of such training was not delivered in the teachers' native Russian language, which limited its impact.
- When asked to receive additional cybersecurity training, 62.5% responded "maybe", while only 18.8% gave a clear "yes" or "no". This hesitancy underscores a need for more accessible, relevant, and engaging formats, particularly those that address linguistic barriers and practical application. This information shows also the lack of time that educators are willing to spend on any extra training, not required by the school itself.
- A key finding is that 85% of participants preferred Russian-language materials. Additionally, those who had received training in a foreign language consistently reported that native-language instruction would improve comprehension and efficiency.
- Post-training survey reveals that 100% of 6 participants who completed it reported increased interest in cybersecurity. Many gained confidence in identifying phishing attacks (50%), scanning suspicious files (66.6%), and practicing safe data and device habits (100%). This shows that well-designed, context-aware training can significantly boost preparedness, even in a short time frame.

While many school teachers in Ida-Virumaa demonstrate moderate cybersecurity awareness and digital competence, their preparedness is constrained by limited access to formal, Russian-language training materials. The results of this thesis show that targeted, interac-

tive, and native-language training significantly enhances readiness. Addressing language barriers, integrating cybersecurity into teacher education, and fostering local knowledge-sharing networks are critical next steps for sustainable improvement in preparedness.

6.5 Future Work

This section provides information relevant to future researchers, highlighting the limitations of the current work and suggesting potential avenues for improvement.

Future researchers investigating similar topics may build upon this work, as it is publicly accessible online and can be modified using the tools described in Section 3.2 Learning Material preparation. The current scope of this research does not encompass all topics relevant to educators in Ida-Virumaa or other educator groups. Notably, topics identified as pertinent during the research process include cyberbullying and safe web browsing. Given the rapidly evolving nature of the threat landscape, future researchers are encouraged to explore additional emerging issues.

A significant challenge encountered during this study was the diminishing availability of cybersecurity learning materials in the Russian language. The platform “itvaatlik.ee” [14] removed all Russian-language content from its website. Similarly, TargaltInternetis” [15] translated its primary Russian-language page into Estonian and removed certain previously available content. This study identified a scarcity of Russian-language resources created in Estonia, which may suggest that Russian-language materials are perceived as less relevant. However, this assumption is contradicted by the findings of this research, which indicated that 85% of the 39 participants expressed a preference for receiving training in their native language. During this research was found that 21% would prefer Estonian as the language for instruction which shows promising results of the current Estonia transition into an Estonian-only education system. Further investigation with a larger sample size is recommended to better understand the evolving demand for Russian-language training materials and the changing linguistic dynamics over time.

7. Conclusion

This thesis explored the development of cybersecurity learning material explicitly tailored for school educators in Ida-Virumaa, addressing the unique challenges of this region, including its linguistic and cultural diversity. The primary goal was to design an accessible, engaging, and practical training program to raise cybersecurity awareness and provide teachers with the necessary skills to protect themselves from cybersecurity threats within school environments.

This is followed by a background section, which includes both practical context and literature review. It was concluded that the current landscape of linguistics within the region and available training in Russian is not enough to prepare teachers for the ever-changing cybersecurity threat landscape. From the literature review, it was concluded that training for school educators is indeed in need. Most preferable methods of education explored. Afterward, the most essential cybersecurity threats within the school were discussed.

The findings from the pre-training survey revealed a pressing need for such training, with most teachers reporting limited formal cybersecurity education and a preference for learning material in their native language, Russian. This insight guided the creation of a gamified and interactive learning material designed to address critical cybersecurity topics such as phishing, malware prevention, personal data protection, mobile application restrictions, and secure password practices.

The training program was evaluated through pre- and post-training surveys, which demonstrated a marked improvement in participant's cybersecurity awareness and ability to protect themselves. Participants highlighted the value of interactive methods and gamification, underscoring the effectiveness of problem-based learning in fostering engagement and retention. Localizing content into Russian proved essential in enhancing accessibility and comprehension, ensuring the training resonated with the target audience.

This initiative not only equipped educators with necessary cybersecurity knowledge but also inspired many to act as ambassadors for digital safety within their schools, fostering a culture of cybersecurity awareness. This project contributes to the broader goal of enhancing digital resilience in educational institutions by addressing a critical gap in teacher preparedness.

In conclusion, this thesis highlights the importance of tailored, accessible cybersecurity education for school teachers in their native language, demonstrating that targeted initiatives can effectively improve cybersecurity awareness and contribute to a more secure and resilient educational landscape.

References

[1] Education Estonia. *A new chapter in Estonian education: Uniting through instruction language*. [Accessed 01-05-2025]. 2024. URL: https://www.educationestonia.org/estonian-education-language-reform/.

[2] Erwan Beguin et al. "Computer-Security-Oriented Escape Room". In: *IEEE Security and Privacy* 17 (July 2019), pp. 78–83. DOI: 10.1109/MSEC.2019.2912700. URL: https://doi.org/10.1109/MSEC.2019.2912700.

[3] Ge Jin et al. "Game based Cybersecurity Training for High School Students". In: *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. SIGCSE '18. Baltimore, Maryland, USA: Association for Computing Machinery, 2018, pp. 68–73. ISBN: 9781450351034. DOI: 10.1145/3159450.3159591. URL: https://doi.org/10.1145/3159450.3159591.

[4] Willi Lazarov et al. "Interactive Environment for Effective Cybersecurity Teaching and Learning". In: *Proceedings of the 18th International Conference on Availability, Reliability and Security*. ARES '23. Benevento, Italy: Association for Computing Machinery, 2023. ISBN: 9798400707728. DOI: 10.1145/3600160.3605007. URL: https://doi.org/10.1145/3600160.3605007.

[5] Gabriele Costa et al. "Why Mary Can Hack: Effectively Introducing High School Girls to Cybersecurity". In: *Proceedings of the 18th International Conference on Availability, Reliability and Security*. ARES '23. Benevento, Italy: Association for Computing Machinery, 2023. ISBN: 9798400707728. DOI: 10.1145/3600160.3605009. URL: https://doi.org/10.1145/3600160.3605009.

[6] Michael Allen. "Leaving ADDIE for SAM: Moving Beyond Content-Centered Design". In: [Accessed 16-01-2025]. Sept. 2012. ISBN: 978-1562867119. URL: https://content.alleninteractions.com/hubfs/eBooks%20-%20White%20Papers%20-%20Case%20Studies/White-Paper-Allen-Interactions-Leaving-ADDIE-for-SAM-Beyond-Content-Centered-Design.pdf?hsCtaTracking=006ca52b-715f-4219-8da1-a991264e2c07%7Ce15a6110-1d4c-4b06-9ee7-514b20c28319.

[7] UNDP (United Nations Development Programme). *National Human Development Report Estonia: 2012/2013*. https://hdr.undp.org/system/files/documents/2013nhdrestonia.pdf. [Accessed 11-11-2024]. 2013.

[8] Statistics Estonia. *RL214492: POPULATION BY COMMAND OF LANGUAGE, SEX, AGE GROUP, AND PLACE OF RESIDENCE (SETTLEMENT REGION), 31 DECEMBER 2021*. [Accessed 16-04-2025]. 2022. URL: https://andmed.stat.ee/en/stat/rahvaloendus__rel2021__rahvastiku-demograafilised-ja-etno-kultuurilised-naitajad__voorkeeleoskus-murded/RL214492.

[9] Statistics Estonia. *RLV003: POPULATION BY PLACE OF RESIDENCE (SETTLEMENT), SEX AND AGE GROUP (2000, 2011, 2021)*. [Accessed 16-04-2025]. 2022. URL: https://andmed.stat.ee/en/stat/rahvaloendus__rel_vordlus__rahvastiku_paiknemine/RLV003.

[10] Statistics Estonia. *RL21434: POPULATION BY MOTHER TONGUE, SEX, AGE GROUP AND PLACE OF RESIDENCE (ADMINISTRATIVE UNIT), 31 DECEMBER 2021*. [Accessed 16-04-2025]. 2022. URL: https://andmed.stat.ee/en/stat/rahvaloendus__rel2021__rahvastiku-demograafilised-ja-etno-kultuurilised-naitajad__rahvus-emakeel/RL21434.

[11] Statistics Estonia. *RL21439: POPULATION, 31 DECEMBER 2021 by Year, Age group, Place of residence, Sex and Command of foreign languages*. [Accessed 30-04-2025]. 2022. URL: https://andmed.stat.ee/en/stat/rahvaloendus__rel2021__rahvastiku-demograafilised-ja-etno-kultuurilised-naitajad__voorkeeleoskus-murded/RL21439/table/tableViewLayout2.

[12] Chuiko Roman. *Kiberbezopasnost': pravila dlja uchenika i uchitelja — youtube.com*. https://www.youtube.com/watch?v=RDZxKin3X_w. [Accessed 03-04-2024]. 2019.

[13] Bea Shuster. *Kiberbezopasnost' dlja uchitelej — chto nuzhno znat' v 2025*. https://ru.vpnmentor.com/blog/%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE-%D0%BF%D0%BE-%D0%B2%D0%BE%D0%BF%D1%80%D0%BE%D1%81%D0%B0%D0%BC-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0/. [Accessed 28-03-2025]. 2025.

[14] Riigi infosüsteemi amet. *Obnovljaj - ITVaatlik — itvaatlik.ee*. https://www.itvaatlik.ee/ru/uuenda/. [Accessed 10-09-2024]. 2024.

[15] Lastekaitse Liit. *Dlja uchitelej - Targalt Internetis — targaltinternetis.ee*. https://www.targaltinternetis.ee/ru/%d0%b4%d0%bb%d1%8f-%d1%83%d1%87%d0%b8%d1%82%d0%b5%d0%bb%d0%b5%d0%b9/. [Accessed 10-09-2024]. 2024.

[16] Riigi Infosüsteemi Amet. *Riigi Infosüsteemi Amet NCSC-EE — infosysteemiamet*. https://www.youtube.com/@infosysteemiamet/videos. [Accessed 10-09-2024]. 2024.

[17] Amankwa Eric. "Relevance of Cybersecurity Education at Pedagogy Levels in Schools". In: *Journal of Information Security* 12 (Sept. 2021), pp. 233–249. DOI: 10.4236/jis.2021.124013. URL: https://doi.org/10.4236/jis.2021.124013.

[18] Cleve Hamasaki. "Cybersecurity for middle school teachers". In: (2023). [Accessed 20-05-2024]. URL: https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/1dc6ba06-882f-42b1-a7ea-165d7c0681f2/content.

[19] Sandeep Sarowa et al. "Cyber Security Challenges and Proactive Measures in Education Cyberspace". In: *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*. 2023, pp. 333–337. DOI: 10.1109/InCACCT57535.2023.10141832. URL: http://dx.doi.org/10.1109/InCACCT57535.2023.10141832.

[20] Giti Javidi and Ehsan Sheybani. "K-12 Cybersecurity Education, Research, and Outreach". In: *2018 IEEE Frontiers in Education Conference (FIE)*. 2018, pp. 1–5. DOI: 10.1109/FIE.2018.8659021. URL: http://dx.doi.org/10.1109/FIE.2018.8659021.

[21] Gina Childers et al. "K-12 educators' self-confidence in designing and implementing cybersecurity lessons". In: *Computers and Education Open* 4 (2023), p. 100119. ISSN: 2666-5573. DOI: https://doi.org/10.1016/j.caeo.2022.100119. URL: https://www.sciencedirect.com/science/article/pii/S2666557322000465.

[22] Ruth Shillair et al. "Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise". In: *Computers and Security* 119 (2022), p. 102756. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2022.102756. URL: https://www.sciencedirect.com/science/article/pii/S0167404822001511.

[23] The EdWeek Research Center. *The State of Cybersecurity Education in K-12 Schools | Cyber.org — cyber.org*. https://cyber.org/news/state-cybersecurity-education-k-12-schools. [Accessed 04-03-2024]. 2020.

[24] Bekir Mugayitoglu et al. "A university's developmental framework: Creating, implementing, and evaluating a K-12 teacher cybersecurity micro-credential course". In: Cited by: 0. 2021, pp. 35–40. URL: https://www.scopus.com/inward

/record.uri?eid=2-s2.0-85105867054&partnerID=40&md5=4d3140888267c6189eb1d76ae1c896ad.

[25] Daniel Kahneman. "A Perspective on Judgment and Choice: Mapping Bounded Rationality". In: *American Psychologist* 58.9 (2003). Cited by: 3666, pp. 697–720. DOI: 10.1037/0003-066X.58.9.697. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-0242267471&doi=10.1037%2f0003-066X.58.9.697&partnerID=40&md5=8fb196d0dae13c02b99c6f23e5f384d1.

[26] Zheng Yan, Yukang Xue, and Yaosheng Lou. "Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers". In: *Computers in Human Behavior* 121 (2021), p. 106791. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2021.106791. URL: https://www.sciencedirect.com/science/article/pii/S074756322100114X.

[27] Nabin Chowdhury, Sokratis Katsikas, and Vasileios Gkioulos. "Modeling effective cybersecurity training frameworks: A delphi method-based study". In: *Computers and Security* 113 (2022), p. 102551. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2021.102551. URL: https://www.sciencedirect.com/science/article/pii/S0167404821003758.

[28] Gahangir Hossain, Mikyung Shin, and Mehnaz Afrose. "Empowering K-12 STEM Educators: Enhancing Cybersecurity Awareness Through Professional Development". In: *2024 IEEE International Conference on Consumer Electronics (ICCE)*. 2024, pp. 1–5. DOI: 10.1109/ICCE59016.2024.10444288. URL: http://dx.doi.org/10.1109/ICCE59016.2024.10444288.

[29] Andrzej Pieczywok. "Cybereducation in Society – Benefits and Threats". In: *Studia Iuridica Lublinensia* 33 (June 2024), pp. 299–312. DOI: 10.17951/sil.2024.33.2.299-312. URL: http://dx.doi.org/10.17951/sil.2024.33.2.299-312.

[30] Madhav Mukherjee et al. "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes". In: *Information* 15.2 (2024). ISSN: 2078-2489. DOI: 10.3390/info15020117. URL: https://www.mdpi.com/2078-2489/15/2/117.

[31] Fiona Nah et al. "Gamification of Education: A Review of Literature". In: June 2014, pp. 401–409. ISBN: 978-3-319-07292-0. DOI: 10.1007/978-3-319-07293-7_39. URL: http://dx.doi.org/10.1007/978-3-319-07293-7_39.

[32] Iván Ortiz-Garces et al. “Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions”. In: *Electronics* 12.7 (2023). ISSN: 2079-9292. DOI: 10.3390/electronics12071753. URL: https://www.mdpi.com/2079-9292/12/7/1753.

[33] Matthew Canham, Clay Posey, and Michael Constantino. “Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks”. In: *Frontiers in Education* 6 (2022). ISSN: 2504-284X. DOI: 10.3389/feduc.2021.807277. URL: https://www.frontiersin.org/articles/10.3389/feduc.2021.807277.

[34] Rūta Pirta-Dreimane et al. “CyberEscape Approach to Advancing Hard and Soft Skills in Cybersecurity Education”. In: July 2023, pp. 441–459. ISBN: 978-3-031-35016-0. DOI: 10.1007/978-3-031-35017-7_28. URL: https://doi.org/10.1007/978-3-031-35017-7_28.

[35] Luigi Gallo et al. “The human factor in phishing: Collecting and analyzing user behavior when reading emails”. In: *Computers and Security* 139 (Apr. 2024), p. 103671. ISSN: 0167-4048. DOI: 10.1016/j.cose.2023.103671. URL: http://dx.doi.org/10.1016/j.cose.2023.103671.

[36] Orvila Sarker et al. “A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness”. In: *Journal of Systems and Software* 208 (2024), p. 111899. ISSN: 0164-1212. DOI: https://doi.org/10.1016/j.jss.2023.111899. URL: https://www.sciencedirect.com/science/article/pii/S0164121223002947.

[37] Daniel Jampen et al. “Don’t click: towards an effective anti-phishing training. A comparative literature review”. In: *Human-centric Computing and Information Sciences* 10.1 (Aug. 2020). ISSN: 2192-1962. DOI: 10.1186/s13673-020-00237-7. URL: http://dx.doi.org/10.1186/s13673-020-00237-7.

[38] Fatima Salahdine and Naima Kaabouch. “Social Engineering Attacks: A Survey”. In: *Future Internet* 11.4 (Apr. 2019), p. 89. ISSN: 1999-5903. DOI: 10.3390/fi11040089. URL: http://dx.doi.org/10.3390/fi11040089.

[39] Hossein Abroshan et al. “Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process”. In: *IEEE Access* 9 (2021), pp. 44928–44949. ISSN: 2169-3536. DOI: 10.1109/access.2021.3066383. URL: http://dx.doi.org/10.1109/ACCESS.2021.3066383.

[40] Chulwon Lee and Kyungho Lee. “Impact Analysis of Resilience Against Malicious Code Attacks via Emails”. In: *Computers, Materials and Continua* 72.3 (2022), pp. 4803–4816. ISSN: 1546-2226. DOI: 10.32604/cmc.2022.025310. URL: http://dx.doi.org/10.32604/cmc.2022.025310.

[41] Mohammad Abu Qbeitah and Monther Aldwairi. “Dynamic malware analysis of phishing emails”. In: *2018 9th International Conference on Information and Communication Systems (ICICS)*. 2018, pp. 18–24. DOI: 10.1109/IACS.2018.8355435. URL: http://dx.doi.org/10.1109/IACS.2018.8355435.

[42] Łukasz Tomczyk et al. “How are teachers being attacked online? On cyberbullying and cyberaggression that targets school educators from the student’s perspective”. In: *Online Journal of Communication and Media Technologies* 14.3 (July 2024), e202431. ISSN: 1986-3497. DOI: 10.30935/ojcmt/14602. URL: http://dx.doi.org/10.30935/ojcmt/14602.

[43] Beate Grawemeyer and Hilary Johnson. “Using and managing multiple passwords: A week to a view”. In: *Interacting with Computers* 23.3 (2011), pp. 256–267. DOI: 10.1016/j.intcom.2011.03.007. URL: http://dx.doi.org/10.1016/j.intcom.2011.03.007.

[44] Fariza Khalid and Tewfiq El-Maliki. “Teachers’ Experiences in the Development of Digital Storytelling for Cyber Risk Awareness”. In: *International Journal of Advanced Computer Science and Applications* 11.2 (2020). DOI: 10.14569/IJACSA.2020.0110225. URL: http://dx.doi.org/10.14569/IJACSA.2020.0110225.

[45] Tiziano Citro, Giuseppina Palmieri, and Maria Angela Pellegrino. “Digital Tools, Approaches and Assessment for Cybersecurity Education via Storytelling: a Systematic Literature Review”. In: vol. 3700. 2024. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85195904996&partnerID=40&md5=63571ea873906cfbdbe02b733bf5fae4.

Appendices

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

I Timofei Mihhailov

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Development of Cybersecurity Learning Material for Future and Current School Teachers in Ida-Virumaa", supervised by Kaido Kikkas
   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.

16.05.2025

[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.