Development of Children's Cyber Security Competencies in Estonia

Birgy Lorenz[1(✉)], Kaido Kikkas[2], and Kairi Osula[3]

[1] School of Information Technologies, Tallinn University of Technology, Akadeemia St 15a, 12616 Tallinn, Estonia
Birgy.Lorenz@ttu.ee
[2] Information Technology College, Tallinn University of Technology, Raja St 4C, 12616 Tallinn, Estonia
Kaido.Kikkas@ttu.ee
[3] Institute of Digital Technologies, Tallinn University, Narva Road 25, 10120 Tallinn, Estonia
Kairi.Osula@tlu.ee

Abstract. In recent years, development of digital competencies has become a major task in the education system as various technologies and Internet have become a staple in ordinary classroom. Safety, both in the physical and digital world, is supposed to keep pace with these developments. In Estonia, the new curricula developed for informatics and related subjects include digital safety. In this study, we have looked at the competencies in Grades 4–9. In our study, 10581 students participated from 40% focus group schools, topics were fraud, data, health, freedom, and online reputation. Based on the results, we will outline the threat groups that the schools and teachers should focus on in Estonia and others that have been overstressed by the awareness training so far. These results will hopefully help to develop better learning materials and tests for Grades 4–9 in order to improve their digital safety competencies.

Keywords: Digital safety · Cybersecurity · Digital competencies
Children's digital skills

1 Background

Digital competency training is an important part of the modern information society. Students are increasingly bringing their own devices to school; schools are provided with high-speed Internet connections, materials be developed for e-learning. At the same time, European countries are still discussing what and how to teach, will it be optional or compulsory, and whether the focus should be on coding or overall digital literacy [16]. They also make a recommendation to deal separately with informatics and digital literacy - the former being part of STEM education and taught by informatics education professionals, and the latter being part of the overall skill set needed to function in a modern society, focusing more on principles and practices of using technologies effectively, safely and ethically.

P. Zaphiris and A. Ioannou (Eds.): LCT 2018, LNCS 10925, pp. 473–482, 2018.
https://doi.org/10.1007/978-3-319-91152-6_36

In 2013–2017, several updates of the DigComp model (Framework for Developing and Understanding Digital Competence) in Europe have been published, focusing on five competency areas: information and data literacy, communication and collaboration, digital content creation, safety, problem-solving. The goal is *to create and edit digital content, to improve and integrate information and content into an existing body of knowledge while understanding how copyright and licenses are to be applied, and to know how to give understandable instructions for a computer system* [1].

Regarding digital safety, the schools have not been regulated by the government more than any other institutions. There have been some initiatives to help the schools to understand the importance of helping teachers and students to be safer when using social media, technical tools, and bring-your-own-device. Examples include the EU European Schoolnet provided E-safety Label and Safer Internet project running in most of the countries [3]. The challenge is that participation in these programmes is optional - those who already understand the value are involved, while those who actually need the programmes can just ignore them (and at first, nothing bad will happen).

1.1 Discussions and Current Practices from Estonia

To analyze schools readiness for digitalization and changed learning Tallinn University has developed a school innovation and digitalization-analyzing tool called "DigiMirror". The tool is used by most of the schools in 2016 to get funding for laptops or desktops from government programs. While there were some questions about digital safety, it was not the focus [9]. In Estonia, there is also a support initiative called the WebPolice that strives to help the public in digital challenges and cybercrime cases, hoping that these recommendations would raise the general awareness [14].

Studies of digital competencies involving Estonian curricula show clear differences between schools - there are institutions that provide good digital literacy skills and there are ones that ban technology from the classroom [15]. Some schools are teaching searching for online information, gathering, analyzing and sharing data as well as developing content. However, when it comes to safety, the main challenge is to grasp that it is everyone's (teachers, students, parents) responsibility, not only a matter for IT managers or teachers of informatics. The study also showed that schools in Estonia vary a lot by the level of equipment they possess, topics they teach, awareness they possess and students they involve - the lack of consistency does not allow us to state that every child in Estonia will get the best digital skillset from the education system. The evaluation of current situation has also been rather poor. The same results came by in the 2014 "DigiTurvis" report where different curricula were analyzed regarding digital safety and cybersecurity topics [11].

Two significant documents have been published in Estonia - the curriculum suggestions for Grades 1–9. In the basic school curriculum, the new emerging topics are coding, multimedia, and cyber hygiene. For example, in Grades 1–3 it is called Digital Safety, in Grades 4–6 Digital Hygiene, in Grades 7–9 Cyber Hygiene) [5]. On the gymnasium level,a new cybersecurity course called "Information Society and Personal Protection" [2] gives hope that safety is going to be focused on more than before. Both of these curricula are developed by education and cybersecurity experts, the digital safety section got insights from the thesis by Lorenz [10].

For 10 years, there have not been any digital competencies testing in Estonia addressing real skills with realistic exercises. For example, when large studies like PISA test IT-related skills, they use 10–20 questions that only measure the student's attitude towards the use of technology, not actual skills. In addition, the questions state attitudes towards specific situations like using technology in free times or doing specific tasks like learning math [13].

Estonia has introduced the DigComp model as a part of the Estonian Students ICT competencies framework since 2016 [4]. As this framework operates as a guideline and is not empirically tested, a toolkit should be developed for teaching and evaluate the results (e.g. testing the skills). There were also attempts to test skills according to the DigComp model in 2016 (pilot study) by Tallinn and Tartu University, but they were likewise focusing on attitudes and functional reading skills rather than IT skills needed to perform the tasks. The positive result of this was that they now know that the DigComp model in its current form is not the way to go (changes are needed both in the model and the questions). Mäeots [12] proposed an update to the current model including the base of information and data literacy, three pillars - communication and collaboration, digital content creation, and safety - and the roof of problem-solving. E-testing is good for gathering a lot of data in a short amount of time, but before testing, we should also set the baseline what is the knowledge that the students currently possess regarding digital literacy. At the same time, the teachers' digital competency model relies on ISTE. The ISTE standards focus on learning, teaching, and management in the digital age [6–8] and are different in some parts compared to the needs of the students' skill set.

There has been some effort to develop a national test for digital competencies, but it does not focus on digital safety, rather targeting information literacy, communication, and collaboration. There has been some effort to collect data from schools that have understood the need for it (the topic has been present in some Master and Ph.D. theses). Some practical testing has been done at technology fairs and other events for children, carried out by the Information Technology Foundation for Education, but it has only involved about 400–600 students. Besides, their goal has been rather to promote awareness in the field than to carry out research.

As there has not been any digital safety testing (on any deeper level), in this study we wanted to mark down the baseline for digital safety testing - to understand students' attitudes towards digital safety, to outline the current practices and knowledge taught by the adults (teachers and parents); and to find out who needs the most help in this matter (and what are the most urgent topics). The goal is to develop guidelines for designing a proper digital safety competency-testing tool to show the behavior of the test group in real situations.

2 Methods

In this study, we have looked at the competencies in Grades 4–9, based on the DigComp [1], new curricula topics and the Ph.D. thesis by Lorenz [10]. We allowed everyone to participate in the nationwide study by using an online questionnaire (LimeSurvey). The study was announced to the schools twice and it was available

online for one month in autumn 2017. The focus group consisted of 77 000 students from 493 schools the confidence level was proposed to be 95% with interval ±2 if at least 8539 students participated. The study consisted of 46 questions: 16 for background and 30 for digital safety topics in the areas of fraud, data, health, freedom, and reputation. The difficulty was basic/intermediate, in accord with the national curriculum goals for the age group. The question types used were yes/no, multiple choice, Likert scale, ranking, and topics. The study questions (in Estonian) are available at https://goo.gl/wkb5a2.

The results show 10581 students participating from 40% of the focus group schools; the gender distribution was roughly equal. 53,6% of Grades 4–6 and 46,4% of 7–9 took part in the study. As the response of any group of students depended mainly on their own interest in the matter, we were asking teachers to participate with the whole school or class, to avoid the situation where the respondents are only the students who are better in digital safety and informatics.

The data was analyzed using SPSS for Windows 24.0 and Excel 2011, analyzing the data and interpreting the results' frequency tables and cross tables, charts, descriptive statistics, and correlation. Statistically significant differences between groups were tested by t-test and ANOVA in the level of significance 0.05. As there were no findings of sub-groups from previous studies, we focused on 9 sub-categories according to the topics. The sub-category topics were internally consistent - the value of the Cronbach's alpha was 0.801.

Based on the results, we will outline the threat groups that the schools and teachers should focus on in Estonia and others that have been overstressed by the awareness training so far. These results will hopefully help to develop better learning materials and tests for Grades 4–9 in order to improve their digital safety competencies.

3 Results

3.1 Background Information

Access to technology at homes is far better than at schools - 97% have their own smartphone, use PC or laptop, and have a tablet (66%). Bring Your Own Device (BYOD) is allowed in 72% of schools (in-class, 42%). Every week, students use different devices in schools, but mainly in a computer or extracurricular technology lessons (half of the students are exposed to them). There were schools that tend to ban technology during class time as they see it as a disturbance. Also, the problem is that due to limited resources, technology lessons are only provided to younger students while only 20% of 7–9th-grade students are provided computer lessons with a qualified teacher (as opposed to anyone capable using a computer). Those who participated in computer lessons or extracurricular activities were giving more right answers than others ($p < 0,05,\ t(10579) = 2,04$). Also, age seems to be a factor as older students got better results in digital safety and "security-conscious behavior" ($r = 0.24$).

Attitudes Towards Digital Safety

Most students (91%) state that they have quite good ICT skills. Depending on the school regulations, events involving digital safety are provided to them at least twice

every year (64%), sometimes every month (24%). The events can be anything from just warnings to actual complaints to hands-on workshops. Home support for digital safety is not so high, 42% of parents talk about it only once a year or not at all (24%). 42% of students state that digital safety is not something they discuss with their peers. Students' skills in using appropriate vocabulary and understanding of terms used in the field are lacking, e.g. 35–40% of 4th and 5th-grade students do not understand the meaning of "identity theft", not to mention more complicated terminology.

Safe use of technology means to 26% of students having critical attitudes towards downloads (files, programs), 23% mentioned installing antivirus, 7% having a backup. 32% think all the previous points are vital for safer technology use. Boys tend to stress having an antivirus. Youngers students are less knowledgeable - 19% of 4th graders were unable to answer the questions due to lack of skills or understanding.

3.2 Current Practices and Knowledge Taught by the Adults

Safe Use of Technology

In the study, we presented students with situation awareness questions like "which website to use when their names are similar" or "what to do when an advertisement of antivirus appears to browser or app". All the questions showed around half of the 4th graders taking the wrong road, while only 20% of 7th-grade participants tended to take more risky options. There is more attention when the situation is not so common, but as websites use advertisement and pop-ups in abundance, the students get their awareness dulled. 41% of the younger students hope to receive help in this matter. 14% would download the suggested file or call to the provided 'hotline'.

As access to the internet is vital for these age groups, we asked to pick the safest WiFi network in the shopping mall. 56% of the students took the riskier of familiar ("home network") options, especially students from smaller and rural schools. Distinguishing phishing attempts from other mail is starting to be common knowledge, but 11% of students are willing to start a conversation with the sender to acquire more information or just have fun.

Using mobile devices securely is something that every child is interested in, yet most of them fail to follow simple regulations: 34% of students do not use password, PIN or other lock on their devices. 75% know that deleted files can be restored, but only 36% think that destroying the medium is the only way to destroy data on it. The students have no skills to deal with ransomware - they suggest asking help from the web police, then try to use hackers, propose a deal to the criminals to share the malware with others when their files are opened for free etc. The same goes with attitudes toward illegal downloads – 1/3 is against and 1/3 for shutting down the internet connection when illegal files are downloaded.

Students are also pushed to use cloud services, the most popular being Google. The reasons for using Google services are the most popular devices being Android smartphone, getting some disk space for free, possibility to use it for authentication to another service (e.g. social media or educational services) and extra services like a spam filter and antivirus.

Behavioural Factors
Sharing personal information and attempting to build a positive image of oneself online has a positive outcome - students know what is considered good behavior by the adults. When something happens the most popular person to turn to is Web police, parents or a local 'IT guru'. On the other hand, a chance to get help from peers is lower than ever, that applies also to cyberbullying situations. Expecting that others (adults, officials) will react when something bad happens and deal with the situation themselves; the youth tend to be reactive. 21% of students would not intervene in a situation and 9% state that it doesn't matter if they do it or not.

Overuse of technology (sometimes called 'addiction') is also considered a part of digital safety. Seems that no one really knows what it is, yet everyone worries about it. The results show lack of understanding - it seems that adults are trying to control children behavior with fear or by discrediting them.

There is also social pressure from peers to be part of the community, stay up late, and take up challenges as soon as they appear. Another matter is cyberbullying that needs more attention from parents - we will address this in the discussion below.

4 Discussion

The students' answers show their basic skills in managing their online presence (sharing positive content, not sharing personal information), but there is lack of understanding what to do in more difficult cases. For example, some tools provided by the service providers are used by some, for others, the main obstacles are lack of knowledge, laziness and the belief that nothing bad will happen online. Everyone seems to know that viruses are a part of digital life, yet when prompted with a name or a suggestion to use a "better" program, younger students still fall into the trap (as well 20% of older students). The situation is better in using mobile devices as the actual experience level seems to be higher than at using the computer. Heavy gamers seem to be the most knowledgeable among students, but gaming itself is seen "the way to computer addiction" by adults. Students are affected by easy pranks and cheat like fake websites or apps, or an insecure Wi-Fi network (phishing). Younger, less experienced students (4th–5th graders) are more in need of help, likewise students from the rural areas and smaller communities due to their lack of people capable of identifying and explaining bad behavior.

When a problem occurs, the solution seems to be to run for help, sometimes turn immediately to the web police (who should be a higher level of assistance when local measures do not help). As a result, the web police is overburdened with basic problems that could be solved involving parents, local IT experts or other local means. An example: when a student sees a street accident, he/she would first send an SMS to parents and then open up the Facebook to ask help from friends. When the friends advise calling the police, the student would ask someone else from the screen to do it for him/her. Then she/he would leave the scene as all that he/she could do is done.

Schools need help with developing guidelines or strategies how to help students to remember the solutions for basic problems. For now, schools are regulating the time spent with technology (sometimes banning technology from the school) and stressing

positive content use and creation, but students are not covered outside the school premises where they are supposed to be self-managing. As the cyberbullying is still part of Estonian children's everyday life, there is also need to help them with their self-esteem, dealing with social pressure etc. We feel that this cannot be done without involving parents remarkably more than this has been done so far.

Because of all this, we cannot agree with the presumption that students are ready for the digital world, or possess a higher cyber hygiene level than adults.

4.1 Recommendations for Local Authorities and Officials

In Estonia, schools are governed by local authorities, the Ministry of Education and Science and private institutions (e.g. foundations). Our results show significant disorder when it comes to digital safety - in some schools, there are functional lessons with an appointed supervisor, in some schools supervisors lack suitable background (the person is appointed but is unable to perform) and in some places, we met overall ignorance about digital safety. Other studies like CECE show the similar picture in the EU, and there are significant differences between countries as well.

The situation will not improve when digital safety at school is just one person's responsibility; instead, we should strive for a certain general level of awareness among all parties involved (school personnel, parents, support specialists etc.). To advance further, informatics should be changed in curriculum from optional to mandatory, testing the school's results on digital literacy should be introduced and it should focus on behavior in real situations (via e.g. practical simulations) rather than just attitudes.

4.2 Recommendations for the Schools

One of the biggest challenges is dealing with cyberbullying - getting it into everyone's view as something they cannot ignore, encouraging victims to talk and ask for help, collecting evidence (logs, screenshots, and timestamp) etc. Peer pressure is a real issue - for example, there was a case of an online community where the administrators gave out orders to complete various "tasks" - including walking in the street blindfolded, running across the streets defying cars, cutting oneself in the face etc.; the ultimate task was committing suicide.

There is also a need for common solution models for most of the challenges. For now, students and teachers tend to seek help from the web police at once, instead of looking for an easier solution at hand. In Estonia, the web police only consists of 4 people who are overburdened with problems that could actually be solved by just talking to each other. This kind of class or school level challenges must be solved within the institution involving parents, teachers and other professionals like psychologists, IT personnel, teaching manager etc. Only the second phase (if needed) would be asking help from outside (police, child welfare or other services).

In the area of informatics being taught, the curriculum topics must also include safe use of mobile devices - how to change one's password/pattern and what would be the best ones to use, how to turn in location service for one's phone to look it up when it gets lost. Social media tools should be used to report inappropriate content or remove inaccurate results from a search engine (the EU "right to be forgotten" legislation).

There is still lack of understanding why and which antivirus and firewall to use, how digital data is destroyed etc. Accurate study materials regarding critical thinking and social manipulation are needed as well as practical (yet safe) experiments of being a victim of phishing by accessing public Wi-Fi networks or even receiving emails and other messages.

It is also important to address the use of cloud services. When there is no regulation what service to use then it should be chosen more freely - the solution is not just to direct students to Google. We understand that when most students have an Android-based smartphone, Google would be the most popular e-mailing service, but nevertheless, not everyone agrees with their user agreement and privacy regulations, so it cannot be mandatory. Most schools tend to start using cloud services like Google Education or Office 365 as the benefit is a built-in spam filter, unlimited space, possibilities to use it as justification tool etc. When providing official mail service to the students then it cannot be provided without the consent of the parents. Either way, the students should learn how to use multifactor authentication and identity management (e.g. using different personas in a different context - one account/persona for school, another for social networks etc.).

4.3 Recommendations for the Family

A major role of parents is setting the boundaries and values. Families must discuss what is and what is not private information - is location, daily schedule, academic performance or even the name of the family pet something we should reveal to the world, or does it have risks involved (e.g. accounts can be taken over due to easy-to-guess answer to the password remembering question). Also, they should learn to distinguish online personas from real-life persons (e.g. many people tend to create an idealized picture of themselves, making online environment a kind of virtual theatre rather than a place to discuss different issues and solve actual problems).

5 Conclusion

Our current study was done by e-testing. This method has its limitations – it allows us to study behaviors and attitudes, but not real practical skills and behavior in real situations. A sizable number of schools agreed to participate in the study, so it shows interest and readiness from schools to start dealing with the situations (that have become part of everyday life by now). The problem is that as Estonia is often seen as one of the leading digital nations and according to a cliché, “we believe firmly in freedom and autonomy”, we do not have other countries to learn from - and the constant developing of ‘our own way’ can lead to new problems. From the study, we understood that the biggest factor is again to start to educate all teachers and adults who influence the youth, as in serious situations, students still look upon adults for a solution. The schools need basic strategies or guidelines how to solve common cases and teach that to all of the school community (students, teachers and parents). This will ease the work of web police and other institutions. A tool should be developed to simulate an incident and measure the consequences - this is again needed both by

students and adults. It is also necessary to involve different language and cultural groups (e.g. Russian speakers in Estonia) to this process, even if it has proven difficult.

Acknowledgements. This research was supported by the Republic of Estonia Ministry of Defence program support of Cyber Olympic.

References

1. Carretero, S., Vuorikari, R., Punie, Y.: DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use (No. JRC106281), Joint Research Centre (Seville site) (2017). https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-21-digital-competence-framework-citizens-eight-proficiency-levels-and-examples-use. Accessed 25 Jan 2018
2. Estonian Atlantic Treaty Association: Valikõppeaine "Küberkaitse" ainekava, EATA (2017). https://1drv.ms/w/s!AuRLzcD9FVl7ywlqPX-J4ewoLgIy. Accessed 25 Jan 2018
3. European SchoolNet: E-Safety Projects, European Schoolnet Online (2012). http://www.eun.org/about/projects/esafety. Accessed 25 Jan 2018
4. HITSA: Õppijate Digipädevuse mudel. Innovatsioonikeskus.ee (2016). http://innovatsioonikeskus.ee/sites/default/files/Digipadevused/Digipadevusmudel_2016.pdf. Accessed 25 Jan 2018
5. HITSA: Kontseptsioon "Uued õppeteemad põhikooli informaatika ainekavas nüüdisaegsete IT-oskuste omandamise toetamiseks", HITSA (2017). https://drive.google.com/file/d/0B1-0pZFgjFnQX29Gb0ZYb1FMc0k/view. Accessed 25 Jan 2018
6. Iste.org: ISTE Standards for Students, ISTE (2007). http://www.iste.org/standards/iste-standards/standards-for-students. Accessed 25 Jan 2018
7. Iste.org: ISTE Standards for Teachers, ISTE (2008). http://www.iste.org/standards/iste-standards/standards-for-teachers. Accessed 25 Jan 2018
8. Iste.org: ISTE Standards for Computer Science Educators, ISTE (2011). http://www.iste.org/standards/iste-standards/standards-for-computer-scienceeducators. Accessed 25 Jan 2018
9. Laanpere, M.: Digital Mirror: a framework and Web tool for assessing the school's digital maturity, ERA Chair project CEITER (2016). http://ceiter.tlu.ee/digital-mirror-a-framework-and-web-tool-for-assessing-the-schoolsdigital-maturity. Accessed 25 Jan 2018
10. Lorenz, B.: A Digital Safety Model for Understanding Teenager Internet Users Concerns, Tallinn University (2017). http://www.etera.ee/zoom/30536/view?page=1&p=separate&view=0,0,2067,2834. Accessed 25 Jan 2018
11. Lorenz, B., Laanpere, M., Laugasson, E., Püvi, D.: DigiTurvis - uuringu aruanne, Tallinna Ülikool (2014). onedrive.live.com/view.aspx?resid = 120A5B9B56F334F2!340&ithint = file%2cdocx&app = Word&authkey = !ALtyGq2CQwFt7Q4. Accessed 25 Jan 2018
12. Mäeots, M.: Development of electronic tools and methodology for the assessment of digital competency for the graduating classes of basic and upper secondary schools, project financed by Ministry of Education and Research, meeting slides Tallinn University, 8 November 2017
13. OECD: PISA 2015 Results (Volume III) Students' Well-Being Students' use of ICT outside of school (2017). http://www.oecd-ilibrary.org/education/pisa-2015-results-volume-iii/students-use-of-ict-outside-of-school_9789264273856-17-en. Accessed 25 Jan 2018
14. Police and Border Guard: Veebikonstaablid annavad internetis nõu (2015). https://www.politsei.ee/et/nouanded/veebikonstaabel. Accessed 25 Jan 2018

15. Praxis: IKT-haridusest: digioskuste õpetamine, hoiakud ja võimalused lasteaias ja üldhariduskoolis, Hitsa.ee (2017). http://hitsa.ee/ikt-haridus/uuringud/ikt-haridusest-digioskuste-opetamine-hoiakud-ja-voimalused-lasteaias-ja-uldhariduskoolis. Accessed 25 Jan 2018
16. The Committee on European Computing Education (CECE): Informatics Education in Europe: Are We All In The Same Boat? ACM, New York (2017). ISBN: 978-1-4503-5361-8