A novel methodological approach for learning cybersecurity topics in primary schools

Maja Videnovik[1], Sonja Filiposka[2], Vladimir Trajkovik[2]

[1]*Center for Innovations and Digital Education Dig-Ed, Solunska glava br.3, 1000, Skopje, North Macedonia*

[2]*Faculty of Computer Science and Engineering, Ss Cyril and Methodius University in Skopje, Rugjer Boshkovikj 16, 1000, Skopje, North Macedonia*

Corresponding author: Maja Videnovik, +38970585920, maja@dig-ed.org, https://orcid.org/0000-0002-9859-5051

Sonja Filiposka

sonja.filiposka@finki.ukim.mk, https://orcid.org/0000-0003-0034-2855

Vladimir Trajkovik

vladimir.trajkovik@finki.ukim.mk, https://orcid.org/0000-0001-8103-8059

Short biography:

Maja Videnovik is a PhD student at the Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University in Skopje. She is an engineer of informatics and a professor of informatics in primary school, teacher trainer on different topics concerning innovative use of the ICT in education, local expert for development of standards and professional competences for teachers, teacher mentors and teacher advisers and an external associate of the Bureau for Development of Education. As a member of NGO "Center for innovation and digital education", she is interested in using ICT for creating engaging learning environments and integration of educational games in the learning process.

Sonja Filiposka is a full professor at the Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University in Skopje. Since obtaining her PhD in 2009 from the Faculty of Electrical Engineering and Information Technologies she has been actively taking part in a number of research projects related to e-infrastructure, networking and ICT education. During her professional carrier she has authored over 100 research papers published in conference proceedings and journals. Her main research fields of interest include e-services, orchestration of systems, complex networking and security.

Vladimir Trajkovik received Ph.D. degree in 2003 from Ss. Cyril and Methodius University in Skopje. His current position is a professor at Faculty of Computer Science and Engineering. He has published 4 books as author or editor, 16 chapters in different books published by international publishers, as well as more than 60 respectable journals and more than 160 conference papers, having more than 2000 citations, with h-index of 22. Prof. Vladimir Trajkovik, has participated or coordinated in more than 60 national and international ICT projects related to providing novel ICT based services. He is co-founder of two NGOs that promote digital education and usage of ICT in education.

A novel methodological approach for learning cybersecurity topics in primary schools

Abstract

Teaching cybersecurity in primary education can equip students with the knowledge and skills to maintain online safety and establish positive digital behaviours from an early age. Traditional teaching methods are not effective in engaging students in this subject. Hence it is important to adopt innovative, interactive techniques that can sustain students' attention, participation, and openness to discussions.

This paper aims to introduce a new method for teaching cybersecurity in primary schools that blends peer learning with game-based learning. This combination of approaches can provide an engaging, interactive, and dynamic learning experience for students, promoting communication and collaboration, and making the learning process more enjoyable.

The effectiveness of our approach was evaluated in five elementary schools, where students from 6th to 9th grade were divided into two groups. The upper-grade students (8th and 9th) demonstrated improvement in their cybersecurity knowledge and skills through their active involvement in creating educational materials, such as lectures and games that were used to teach the lower-grade students (6th and 7th). The evaluation of the approach indicated that students enhanced their cybersecurity understanding and developed critical thinking, communication, and teamwork skills.

Keywords: cybersecurity education, peer learning, game-based learning, digital educational resources, interactive learning environment

1. Introduction

Education in cybersecurity is important because it helps individuals and organizations protect against cyber threats such as hacking, data breaches, and other malicious activities (Rowe et al., 2011). As the digital world continues to expand, the need for cybersecurity professionals will only continue to grow (Blažič, 2022). The changes in cybersecurity education should happen in all educational levels, starting with introduction to positive digital behavior in primary education.

Cybersecurity education in primary schools can help young students develop a strong understanding of how to stay safe online and develop positive digital behavior at an early age. This can include topics such as internet safety, how to identify and avoid online scams, how to protect personal information, and how to be a responsible digital citizen (Suson, 2019). By teaching these concepts at a young age, students will be better prepared to navigate the online world as they grow older and encounter more complex issues. It also helps to build a culture of cybersecurity awareness in the future (Richardson et al., 2020).

Cybersecurity education in primary schools mainly focuses on teaching children the basics of staying safe online, such as creating strong passwords, being cautious about sharing personal information, and identifying potential scams or malicious software (Kaban, 2021). This education also includes lessons on responsible technology use, such as avoiding cyberbullying and respecting online privacy (Martin et al., 2019).

There are still a number of challenges that can make it difficult to effectively implement cybersecurity education in primary schools. Some of these include:

- Limited resources: Many primary schools may not have the budget or resources to provide comprehensive cybersecurity education (Javidi & Sheybani, 2019).
- Lack of specialized teachers: cybersecurity education requires specialized knowledge and skills, and many

primary schools may not have teachers who are trained in this area. Many teachers lack knowledge and expertise in cybersecurity and they need more learning materials aligned with the fast technological change (Rahman et al., 2020).

- Keeping up with technology: Cybersecurity threats and technology are constantly evolving, making it a challenge to ensure that curriculum and teaching methods stay current (Aldawood & Skinner, 2019).
- Limited access to technology: In some schools, students may not have access to the technology and internet resources needed to effectively learn about cybersecurity (Rahman et al., 2020).
- Limited parent and community engagement: Parents and communities play important roles in education, and it is important to engage them in cybersecurity education in primary schools (Pencheva et al., 2020).
- Limited understanding of the concept: Cybersecurity is a complex subject, and it can be challenging for primary school students to understand it (Kam & Katerattanakul, 2019).
- Age-appropriate content: It is important to provide age-appropriate content, as primary school students will have a different understanding and maturity level than secondary school or college students (Muir & Joinson, 2020).

In order to address these challenges, different pedagogical approaches have been implemented during cybersecurity education (Kam & Katerattanakul, 2019). The main aim is to establish an interactive and engaging learning environment that will increase students' interest and motivation to develop their competencies in this field. Research shows that different innovative teaching approaches can provide “hands on” and “real life” experiences that greatly enhance traditional classroom teaching (Sağlam et al, 2023). Open discussions, connections to real world situations and learning based on different scenarios are desired learning environments that can lead to successfully integration of cybersecurity in schools (Pencheva et al., 2020).

A strategy that can be used to motivate and engage students in learning is implementing a digital game-based approach. Students, who are digital natives, play games daily with such dedication, so educators must find different ways to use that dedication in the learning process. Game-based education is a teaching method in which educational content is delivered through games and interactive activities, incorporating immersive gameplay into the learning process. Games can make learning more engaging, interactive and thus more effective (Hafeez, 2021).

This approach is often used in primary schools to make learning more engaging and fun for students. Some examples of game-based education in primary schools include using educational games to teach math (Vankúš, 2021) and languages (Lee, 2019) and using board games and mobile platforms to teach science and social studies concepts (Kusuma et al., 2021; Cardinot & Fairfield, 2019). Moreover, online serious games can be used for soft skills assessment, like emotional intelligence (Marengo et al., 2024). Educational games have emerged as a new approach during cybersecurity education that can complement instruction-led or computer-based learning by providing a fun environment (Hart et al., 2020). Research has shown that game-based education can effectively improve student motivation, engagement, and learning outcomes (Sung & Hwang, 2013, Videnovik et al., 2019). Moreover, game-based learning can improve students' competencies and academic performance (Sánchez-Mena & Martí-Parreño, 2017). Educational games promote active and self-directed learning, enabling students to progress through the game at their own pace, through trial and error (Chen et al., 2018; Zhao et al., 2021). Implementation of game-based learning (Olano et al., 2014; Leune & Petrilli, 2017) can enhance the effectiveness of cybersecurity education by creating engaging learning environments that increase awareness of cybersecurity practices. Research show that practical game-based approach can effectively engage students and increase their cybersecurity awareness and skills (Chowdhury & Gkioulos, 2023; Khan et al., 2022; Triplett, 2023).

Despite the great potential of the game-based approach for learning, it must be noted that designing an educational game is a challenging task, having in mind different aspects that should be considered during the design (Hussein et al., 2019). Educational game design means creating meaningful, interactive, and challenging experiences involving the users as self-directors of their learning (Ke et al., 2019). The game should adjust the level of difficulty and

complexity of the content based on the students' performance (Vlahu-Gjorgievska et al., 2018) and provide immediate feedback to the students, so they can understand their progress and adjust their learning strategy accordingly (Zhao et al., 2021).

Peer learning is an active learning strategy that can engage students and make them open in discussions, self-directing their learning. In general, peer learning refers to the students' activities where they can teach and support each other in learning, encouraging them to share knowledge and work together by valuing cooperation rather than competition within the group (Chandra & Palvia, 2021).

The first steps in peer learning were made by Topping (1996), who defined peer learning as the process that occurs when people with similar backgrounds but who are not educators work together and teach one another to understand specific topics. Peer learning is growing internationally as a beneficial pedagogical strategy which enhances students' self-regulated learning (Lim et al., 2020). In the last decade, many researchers have confirmed the effect of peer learning on students' learning and achievement in different areas (Ion et al., 2016; Gamlath, 2022), including cybersecurity education (Deshpande et al., 2019). Peer instruction is useful as teaching method in cybersecurity, bringing relevance of basic concepts closer to the learners and emphasizing practical experiences, overcoming some of the problems caused by different students' backgrounds and experience (Konak, 2018; Scheider & Asprion, 2023). Peer learning can increase students' motivation and engagement in the learning process, inspiring and motivating students for self-guided learning and developing their social skills (Xiao & Lucking, 2008; Nerantzi, 2020). Peer learning also encourages children to take an active role in their education, and this can increase their confidence in their abilities and knowledge (Ädel et al., 2021).

Game-based learning (GBL) and peer learning can be a good combination of teaching approaches when addressing cybersecurity education, since they are promoting engaging, interactive, dynamic learning, fostering communication, collaboration and can make learning more fun and engaging for the students. Furthermore, they can address different challenges that effective integration of cybersecurity education is facing, as presented in Table 1.

Table 1. Challenges to successful implementation of cybersecurity education in primary school and opportunities to address them using GBL and peer learning.

Challenges to effective integration of cybersecurity education in primary school	GBL	Peer learning
Limited resources:		
Many primary schools may not have the budget or resources to provide comprehensive cybersecurity education.	GBL can be run with basic resources	Peer learning can be an effective and low-cost way to provide cybersecurity education, as students can teach each other using resources they already have access to.
Lack of specialized teachers:		
Cybersecurity education requires specialized knowledge and skills, and many primary schools may not have teachers who are trained in this area.	GBL can provide a way for students to learn about cybersecurity in an interactive and engaging way, even if the teacher is not a cybersecurity expert.	Peer learning can provide a way for students to learn about cybersecurity from their peers, even if the teacher is not a cybersecurity expert.
Keeping up with technology:		
Cybersecurity threats and technology are constantly evolving, making it a challenge to ensure that curriculum and teaching methods stay current.	GBL can be easily updated to keep pace with the latest technology and cybersecurity threats.	Peer learning can be an effective way to keep students up to date with the latest technology and cybersecurity threats as students can share their own knowledge and

		experiences with each other
Limited access to technology: In some schools, students may not have access to the technology and internet resources needed to effectively learn about cybersecurity.	GBL can be designed to run on basic technology and can be used in a classroom with limited access to technology.	Peer learning can be done using resources that are available to the students, such as smartphones, making it accessible in a classroom with limited access to technology.
Limited parent and community engagement: Parents and communities play important roles in education, and it is important to engage them in cybersecurity education for primary schools.	GBL can be designed to involve parents and communities, who can play an active role in the game-design.	Peer learning can be designed to involve parents and communities, who can play an active role in the peer learning process.
Limited understanding of the concept: Cybersecurity is a complex subject, and it can be challenging for primary school students to understand it.	GBL can provide interactive and engaging learning experiences that make it easier for primary school students to understand complex concepts like cybersecurity	Peer learning can provide interactive and engaging learning experiences that make it easier for primary school students to understand complex concepts such as cybersecurity as students can explain to each other in a way they understand.
Age-appropriate content: It is important to provide age-appropriate content, as primary school students will have a different understanding and maturity level than secondary school or college students.	GBL can be designed to provide age-appropriate content that is tailored to the understanding and maturity level of primary school students	Peer learning can be designed to provide age-appropriate content suitable for all the participants in the peer learning process

The main goal of this paper is to propose a novel methodological approach for cybersecurity education in primary schools that combines peer learning with a game-based approach.

Proposed methodology for using game-based approach and peer learning during cybersecurity education is described in the next section. Section 3 presents the results from the implementation process and discussion about these results is elaborated in section 4. Section 5 concludes the paper.

2. Methodology

The main idea behind our methodological approach is to increase students' competencies concerning cybersecurity in a fun and exciting way. We wanted to create an interactive learning environment where students would be open to sharing their opinions and talking about possible internet abuse and how to react in that situation. Peer learning was the most suitable pedagogical strategy to create that community of learners. We decided to implement game-based activities to achieve active participation, engagement, and fun during learning. The game-based approach was implemented by learning through designing a cybersecurity game (for upper-grade students) and learning by playing the game (for lower-grade students).

The primary goals of our methodological approach are to:

1. Enhance students' abilities and knowledge in cybersecurity. Upper-grade students search online for information related to cybersecurity, analyze it, discuss, evaluate and make conclusions. Through the peer-

learning approach those students disseminate the gathered knowledge to lower-grade students, start discussions and make conclusions which enhance the cybersecurity knowledge and skills of younger students.

2. Improve students' critical thinking abilities. Students from all grades develop their critical thinking skills by analyzing different information online, evaluating and making conclusions. They also have the opportunity to analyze different types of scenarios and make appropriate decisions.
3. Develop students' digital skills. Upper-grade students develop their digital skills during online searching for useful information, and during the creation of educational resources and that are going to be used afterwards.
4. Identify and address the most challenging topics related to cybersecurity among students. During peer learning through different activities, upper-grade students manage to identify the most challenging issues that lower-grade students are facing and that should be further explained.
5. Promote collaboration and communication among students from different grades. Peer learning activities enable students from different grades to communicate and collaborate among themselves.
6. Increase students' interest and participation in the learning process. Game-based learning as one of the most interactive and engaging activities is expected to increase students' interest and participation in the learning process.
7. Build a community of students who are open to discussing and sharing opinions. Through peer learning activities, an expanded students' community, where they will be open to discuss and share their opinion can be founded.
8. Build a collection of open educational resources (OER) on cybersecurity that can be used freely. Created educational materials and resources are shared online for free and can be used by other teachers and students, as well as other interested parties.

2.1. Methodological steps

The evaluation of our approach was carried out as a case study in five primary schools in North Macedonia. Two teachers from each participating school took part in the activities as facilitators of the learning process. Students from 6^{th} to 9^{th} grade were divided into two groups in the study. The upper-grade students (8^{th} and 9^{th} grade) first enhance their cybersecurity competencies. Then they create educational materials (lectures and games) used for knowledge transfer during lectures given to lower-grade students (6^{th} and 7^{th} grades).

To achieve the primary goals, the proposed methodology for cybersecurity education in primary school was carried out in five steps, as presented in Figure 1.

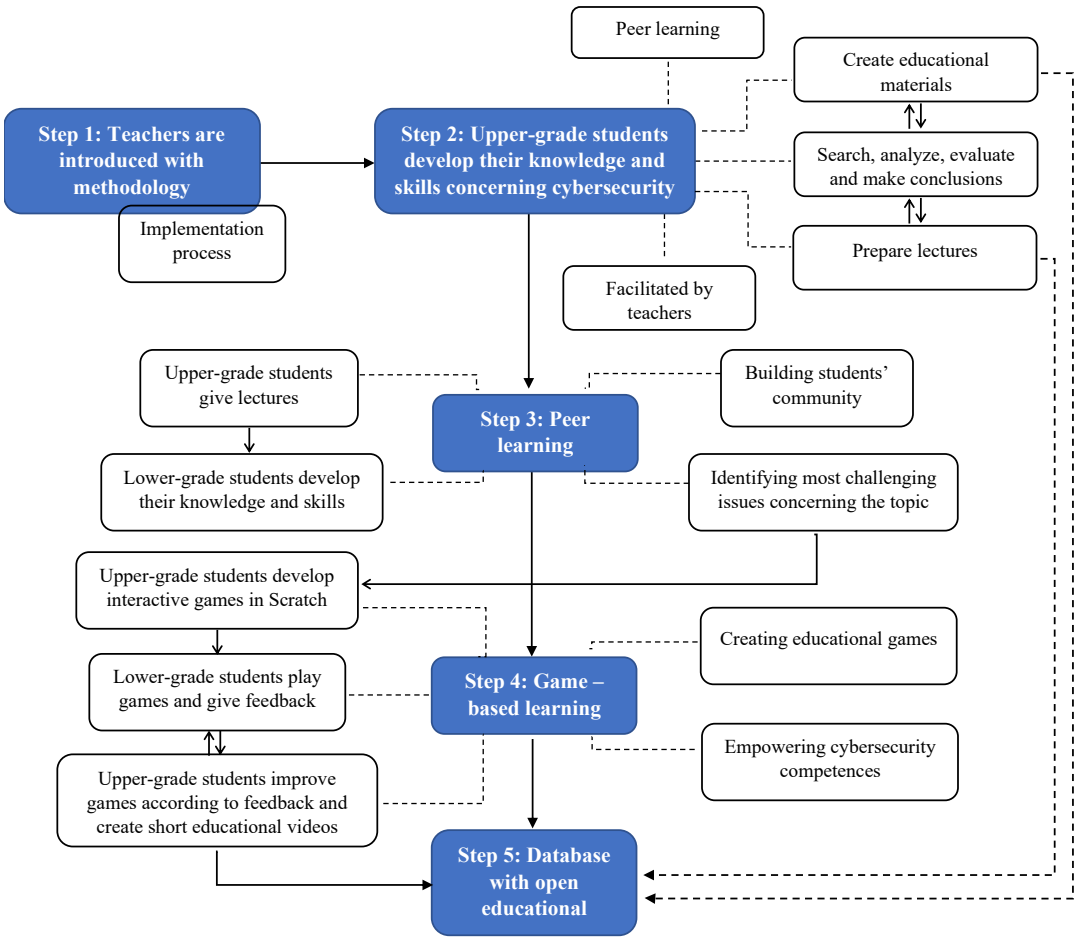

Fig. 1 Proposed methodological approach for implementation of cybersecurity education in primary education

Step 1: At the beginning, teachers were introduced to the proposed methodology for implementing peer learning and a game-based approach to cybersecurity learning. Feedback from teachers, as practitioners, was collected and used to define a timeline for implementing the activities within the case study.

Step 2: The activities in the schools started with empowering upper-grade students' knowledge and skills concerning cybersecurity. Divided into groups, they searched, gathered information, analyzed it and made conclusions on their own. They worked in groups, discussed and learnt from each other. In this way, students developed their critical thinking, communication and collaboration skills. Students created different teaching materials (presentations, videos, quizzes, worksheets) and prepared lectures on cybersecurity. Teachers were facilitators of the activities, monitoring the process and offering help if needed.

Step 3: Peer learning activities were implemented through lectures given to lower-grade students by upper-grade students using materials produced in the previous step. The main aim was to deepen lower-grade students' knowledge and skills related to cybersecurity while initiating discussions and motivating students to participate in them. In that way, a learning community was created. In the end, the most challenging issues on this topic, according to lower-grade students, were identified. The teachers were just organizers of the activity and monitored the work, providing feedback and contributing as necessary. Upper-grade students did all the implementation and guidance during the exercises.


Fig. 2 Examples from implementation of peer learning in lower grades concerning cybersecurity

Step 4: Upper-grade students develop Scratch-based interactive games referring to the most challenging issues concerning cybersecurity identified by students from lower-grade. The game as a resource was used to motivate and engage lower-grade students while enabling them to achieve set of learning objectives (Balakrishna, 2021). Lower-grade students played those interactive games in Scratch, and they deepened their knowledge and skills in a fun and engaging way. After playing, lower-grade students provided feedback about the games, which was used to improve the quality of already created games and to create educational videos on the topic.

Step 5: A set of OER with created teaching materials, interactive Scratch-based games and educational videos was created and shared with free licensing so teachers and students from other schools can reuse it.

2.2. Created educational resources

Different educational resources were created during the implementation of the case study. Teaching materials (learning scenarios, presentations, worksheets and quizzes) were created by upper-grade students, used during the peer learning approach, and improved by students' feedback. Interactive games with questions about the most challenging topics concerning cybersecurity were created by upper-grade students and improved after input from lower-grade students as end users. Educational videos based on those games were recorded in order to introduce users with the purpose of those games and way of playing. All these materials are part of an open educational resources set. The evaluation of the quality of created materials was ensured by the teachers and students that made those materials.

To ensure the accuracy and objectivity of the evaluation, we have included external evaluators in the assessment of the created educational materials. External evaluators were independent experts who could assess the implementation progress and provide feedback, in our case, the academic CIRT (Computer Incident Response Team). It's a group of experts that respond to computer security incidents and provide support, advice, and assistance to organizations and individuals affected by a cyber-attack or other security incident types.

2.3. Methodology evaluation

In order to get quantitative data that can be used to evaluate the effectiveness of the proposed methodology, pre-surveys and post-surveys were implemented with students that took part in these activities. A short pre-survey was conducted to investigate students' previous knowledge of the topic, consisting of a self-assessment questionnaire and a test. The questionnaire was used to self-evaluate students' knowledge and skills concerning cybersecurity, digital skills and skills for creating (using) digital resources. To provide a quantitative measurement of students' perception, which will allow analysis and interpretation of the responses statistically, we have used a 5-point Likert scale, with answers ranging from "I don't have any knowledge/ skill" (1) to "I have excellent knowledge/ skill" (5). It is a very appropriate tool to be used with students in primary school because they can easily understand statements and choose their level of agreement or disagreement with them. For each statement, the mean (on a scale from 1 to 5) and standard deviation (SD) were calculated both for lower-grade and upper-grade students.

The second part of the questionnaire was a short test used to evaluate students' knowledge and skills related to cybersecurity, focusing on fundamental online safety issues that are part of the curriculum in primary schools:

sharing personal information, respecting other people's privacy and identifying insecure links. We have decided to use multiple-choice answers in the test to get quantitative data that can be analyzed more easily, achieving standardization and comparability of students' answers. The answer to each question was scored 1 for correct answer and 0 for incorrect answer. In this way, we managed to compare students' subjective knowledge with the test results. In addition, demographic information about the participants (students' gender, grade and school) was also collected.

In summary, we evaluated the starting point concerning students' knowledge and skills about cybersecurity and collected baseline data (through evaluation and self-evaluation). Additionally, we obtained data to be compared later after implementing the activities envisaged in our approach.

After implementing the proposed methodological steps, a post-survey was conducted in order to collect subjective progress evaluation data. Students' opinions about improvement of their knowledge/ skills as a result of the activities were collected. Five-point Likert scale was used, with answers ranging from "I don't agree at all" (1) to "I completely agree" (5) with the statements about whether those activities have increased students' knowledge/ skills about cybersecurity, digital skills, skills for creating digital resources, as well as critical thinking, communication, collaboration and ability to deliver knowledge during the peer learning process. Information on whether this learning process is more interesting and incite students' engagement was also gathered.

Comparing the data from both surveys, we have managed to assess the effectiveness of implementing peer-learning and game-based approaches during learning topics related to cybersecurity and comprehensively evaluate the achieved results. At the same time, we have identified areas that need improvement and made necessary adjustments for future implementation.

3. Results

3.1. Implementation

Peer learning and game-based learning approaches during cybersecurity education were implemented in five primary schools in North Macedonia (four urban schools and one rural school). The number of students participating in the implementation process depending on the geographical (urban/ rural) and gender (male/ female) distribution is presented in Table 2.

Table 2. Sample distribution

Grade	urban			rural			Total
	male	female	total	male	female	total	
6th	67	70	137	3	1	4	141
7th	51	65	116	3	3	6	122
8th	27	12	39	2	/	2	41
9th	9	23	32	1	2	3	35
Total	154	170	324	9	6	15	339

Two teachers from each of the participating schools were involved and facilitated the activities. The 76 upper-grade students (51,32% male and 48,68% female) and 267 lower-grade students (47,15% male and 52,85% female) participated in the activities. The percentage of students from urban schools is 96,20% from the population of younger students and 93,42% from the population of older students.

All students have already used technology during the educational process, and they have already acquired some digital competences. However, the situation is not the same when it comes to cybersecurity competencies. Only students in higher grades have previously learned cybersecurity topics, so it is expected that they will have better initial knowledge than students from lower grades

For one month upper-grade students deepened their cybersecurity knowledge and prepared educational materials (presentations, quizzes, worksheets, etc.) and lectures for lower-grade students. Lower-grade students learned about cybersecurity topics through lessons delivered by upper-grade students using the already-created educational materials. Those lectures were delivered in the classroom during two classes utilizing a peer learning approach. Provided feedback from lower-grade students was used to create educational games in Scratch by upper-grade students. After one month those games were tested by lower-grade students and their feedback was used to improve them. In this way different game-based learning strategies were implemented: upper-grade students deepen their cybersecurity skills during designing a game and lower-grade students during playing the game. During the whole process, the teacher was just a facilitator, providing feedback to students and ensuring the quality of the implementation.

3.2. Created educational resources

As a result of the implemented approach, students have created educational materials (presentations, quizzes, worksheets), that were used during the peer-learning with lower-grade students. Examples of students' presentations, worksheets, stories and Kahoot quizzes can be seen in Figure 3.

Fig. 3 Examples of educational materials created by upper-grade students

As a result of peer learning and identifying the most challenging cybersecurity issues, students have created interactive games in Scratch concerning those topics. In total, 18 interactive Scratch-based games were designed by the upper-grade students. In this way, they have developed their coding skills and, in parallel, empowered their knowledge concerning cybersecurity. Those games were published online on the scratch.mit.edu platform and can be easily accessed by other students and teachers during their teaching and learning process (Figure 4a). In addition, short educational videos were recorded and put on YouTube as an introduction video for students to play the games (Figure 4b).

External evaluators have checked and provided feedback about the created educational materials. Their feedback was analyzed on an ongoing basis and used to improve the quality of the produced educational resources before publishing.

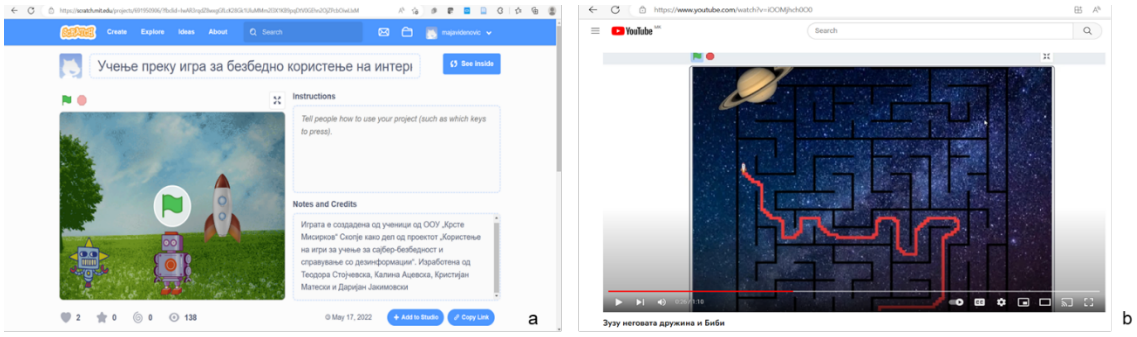

Fig. 4 a) Scratch-based interactive games and b) videos concerning cybersecurity

All created educational materials are shared online (https://dig-ed.org/open-educational-resources/) and are free for reuse by all interested parties on a national level. Additionally, created educational videos could be found on YouTube (http://tinyurl.com/2s3hbmfu).

3.3. Methodology evaluation data

Baseline data marking the starting point of students' knowledge and skills concerning cybersecurity was obtained with short tests (evaluation) and questionnaires for students (self-evaluation). After the implementation, a self-evaluation of the students' improvement as result of this methodological approach was made in order to assess its effectiveness. Upper-grade students have made subjective evaluation of the improvement of their knowledge and skills concerning cybersecurity, digital skills as well as creation of digital content. Similarly lower-grade students made subjective evaluation of the improvement of their knowledge and skills concerning cybersecurity and digital skills. The results from their self-evaluations are presented at Figure 5a (for upper-grade students) and Figure 5b (lower-grade students). The presented self-evaluations were made before (as a baseline) and after the implementation of the approach (as improvement).

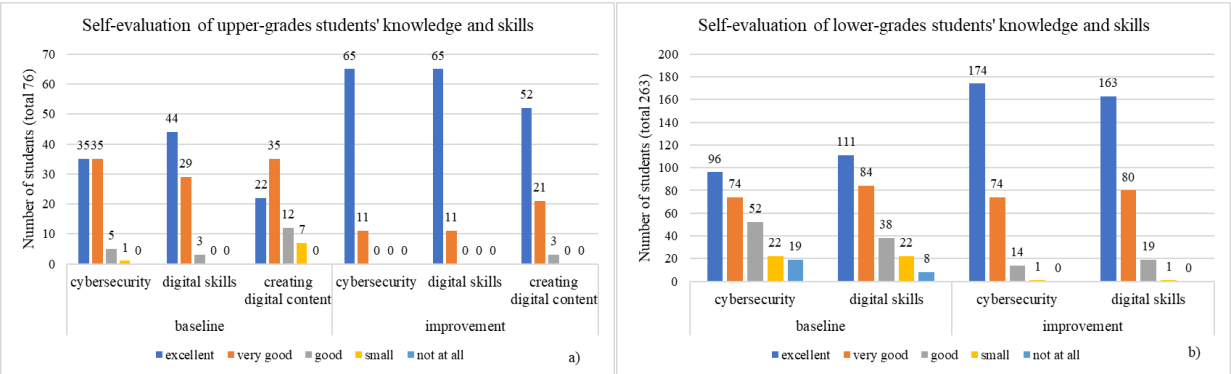

Fig. 5 Students' self-evaluation of knowledge and skills at the beginning (baseline data) and improvement in knowledge and skills as the result of the approach (improvement data) at a) upper-grade students and b) lower-grade students

The results show that before the implementation of the approach, upper-grade students have self-evaluated their knowledge about cybersecurity mostly as excellent or very good and that almost all of them think that they have improved their knowledge during the implementation of the proposed approach. At the beginning the answers of lower-grade students concerning self-evaluation of their cybersecurity knowledge differ among themselves, which was expected because they have never learnt about this topic before. Still, they also think that their knowledge has improved due to the proposed approach. The situation is similar regarding students' digital skills. However, in the beginning, before the implementation of the proposed methodological approach, they evaluated their digital skills better than their cybersecurity knowledge (both upper-grade and lower-grade students). Notably, lower-grade

students' digital skills are initially better than their cybersecurity skills, which is expected since these students have never learned about cybersecurity before. The improvement in digital skills is the same as the improvement in the knowledge about cybersecurity among upper-grade students but is smaller than the improvement in the knowledge about cybersecurity among lower-grade students. The interesting fact is that upper-grade students were not so confident in their skills concerning the development of digital content. Still, they also improved those skills due to the implementation of the activities and the creation of educational resources during the process.

Students' opinion on the effect of the approach's implementation is presented in Figure 6. According to students, the most significant benefit of implementing this approach in cybersecurity education is that the learning process is more interesting than the traditional way of teaching. Most students also think that by implementing peer learning and game-based approaches during cybersecurity education, their critical thinking skills, communication, and collaboration have improved. In addition, upper-grade students think that they have improved their ability to deliver knowledge, and lower-grade students were more engaged due to the proposed approach.

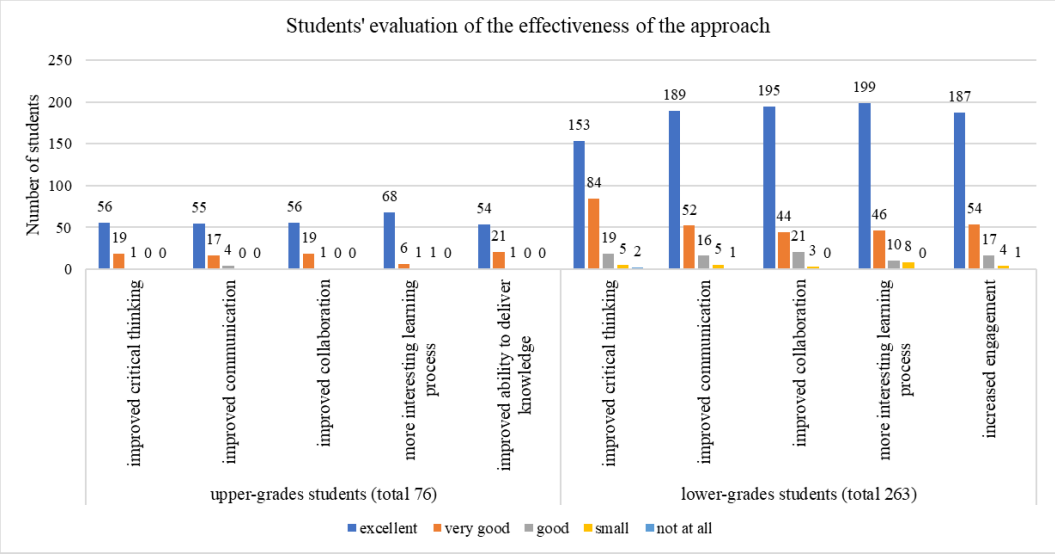

Fig. 6 Students' self-evaluation of the effectiveness of the methodological approach

4. Discussion

The digital natives, being the first generation to grow up in a world where technology is deeply ingrained in their daily lives, have a unique perspective on cybersecurity risks. With their extensive exposure to digital devices and the Internet, they have developed a sense of familiarity with technology that influences their behavior and attitudes towards online security. School has limited impact on their development of secure online behavior. Instead, they mostly learned about it through personal experience, information found on the Internet, guidance from parents and siblings (Witsenboer et al., 2022).

The analyses of results of students' self-evaluation, as baseline data and as improvement data are presented (as an average value of their answers) in Table 3. In the beginning, upper-grade students self-evaluated their knowledge and skills concerning cybersecurity with higher grades (4,37) than lower-grade students (3,78). Although this is their subjective knowledge about cybersecurity it is in accordance with the results from students' evaluations done using a short multiple-choice test. The test results show that, on average, 91,67% of the questions were answered correctly by upper-grade students, and that percentage is lower when lower-grade students (81,75%) answered the questions.

Table 3. Students' self-evaluation of their knowledge and skills before the implementation of the approach (baseline data) and self-evaluation of their improvement as the result of the approach implementation (improvement data)

Students' knowledge and skills concerning	Upper-grade students				Lower-grade students			
	baseline data		improvement data		baseline data		improvement data	
	Mean	SD	Mean	SD	Mean	SD	Mean	SD
cybersecurity	4,37	0,67	4,86	0,35	3,78	1,23	4,60	0,61
digital skills	4,54	0,58	4,86	0,35	4,02	1,09	4,54	0,65
creating digital content	3,95	0,91	4,64	0,56	/		/	

It is interesting that the dispersion of answers from lower-grade students (measured using standard deviation - SD) is much bigger than those of the upper-grade students. This difference in students' knowledge and skills can be expected because upper-grade students have already learned some aspects of cybersecurity in the curriculum, and lower-grade students are introduced to these topics for the first time. The previous knowledge and skills of lower-grade students is the result of their own initiative or interest to learn about the topics (which leads to big dispersion in the results). That is why we have decided that upper-grade students should give lectures, to upgrade their previous knowledge and share with others.

The results connected with the subjective evaluation of students' digital skills are the same. At the beginning upper-grade students have better digital skills than lower-grade students which can be expected due to their longer presence in the digital world and their longer digital education through the years. The smallest self-evaluation was obtained concerning students' ability to create digital content (3,95), and here we have the biggest dispersion of the answers (SD=0,91). This might be a result of the fact that students at their age are not engaged enough in the activities related to the creation of digital content. Some of the students have created digital resources, but the number of students that have very little experience in this field is also significant, which can be a topic of interest in some future research.

The students' subjective evaluation of the improvement shows that upper-grade students perceive that they have empowered their knowledge concerning cybersecurity as a result of the implementation of the approach. Lower-grade students have also stated that they learned something new during the implementation. However, according to their subjective evaluation, their improvement is slightly lower than those of upper-grade students. The values of standard deviation show that the dispersion of students' answers is halved, although it is again bigger than the answers given by upper-grade students.

One possible reason might be that upper-grade students already had better baseline data (had previous knowledge about the topic). The explanation might also be found in the implementation strategy of this methodological approach. Namely, upper-grade students developed their understanding and skills while preparing lectures, designing materials, peer learning, and designing games. This made them active participants, highly engaged, motivated, and persistent during learning, trying to give their best. Lower-grade students progressed through the topic due to learning (during lectures or by playing the game), so each of them progressed according to his interests at his own pace.

The same distribution of the results can be found concerning developing students' digital skills. Upper-grade students had better digital skills at the beginning and progressed more during the process (by creating the different educational resources). As a result of these activities, the most significant progress can be found in students' ability to create digital content. During the approach, the differences among students concerning their ability to create digital content have decreased.

After the implementation, students' subjective evaluation of the development of their critical thinking, communication, and collaboration skills, as the result of the implementation of the approach, is presented in Table 4. It is interesting that upper-grade students again have higher, although insignificant, improvement in their skills

(according to their self-evaluation). The only skill slightly less developed than others is lower-grade students' critical thinking skill, which is not the situation with older students. This can be expected because students from lower grades mainly learned during the participation in lectures, and upper-grade students had to design and deliver those lectures, so they had to carefully analyze all the information, evaluate them, and then make a conclusion. Again, the results obtained for standard deviation confirm the fact that the dispersion of students' answers is bigger among lower-grade students, which can be a result of previously mentioned reasons.

Table 4. Students' self-evaluation of the improvement of their skills as the result of the methodological approach.

Students' skill	upper-grade students		lower-grade students	
	mean	SD	mean	SD
critical thinking	4,72	0,48	4,45	0,77
communication	4,67	0,57	4,61	0,72
collaboration	4,72	0,48	4,64	0,68

Additionally, results from the questionnaire show that upper-grade students think this is a more exciting learning approach (4,86, SD=0,48), and lower-grade students share their opinion on this matter. However, their evaluation of this approach is slightly lower (4,66, SD=0,70). Lower-grade students find this approach engaging (4,60, SD=0,71) by involving them in the activities during peer and game-based learning. The proposed approach also empowered upper-grade students' knowledge and skills to deliver lessons during peer learning.

All previously mentioned can lead to a conclusion that upper-grade students had better knowledge and skills at the beginning of the implementation of the activities. They were also highly engaged during the process, learning by doing and preparing materials, carefully paying attention to how these materials will be created and which information will be presented to lower-grade students. These activities have developed their knowledge connected to cybersecurity, and also empowered their critical thinking, communication and collaboration skills. They have the biggest progress (compared to the baseline evaluation) in the ability to develop different digital resources, and this progress concerned all the participants from upper grades.

At the beginning lower-grade students had less knowledge and skills concerning cybersecurity since they had no previous education on the topic. The distribution of their answers shows that some lower-grade students had already obtained some knowledge of the subject, but that is the result of individual, not organized educational processes.

Subjective evaluation of the approach's effectiveness has shown that all students have empowered their knowledge and skills during the implementation. However, this improvement is slightly bigger for upper-grade students due to their active engagement in designing educational resources. It proves that learning by doing is a highly effective approach for developing students' knowledge and skills. Lower-grade students have also improved their competencies, as a result of this implementation strategy, according to their subjective evaluation. It must be pointed out that there are differences in their answers. Still, this dispersion is halved compared to the baseline data, indicating their progress due to this methodological approach.

Results were also analyzed on the gender differences concerning cybersecurity education. The research has shown that males are more engaged and show higher self-efficacy in cybersecurity (Amo, 2016; Fatokun et al., 2019), and females have more heightened cybersecurity awareness (McCormac et al., 2017; Fatokun et al., 2019). However, analyzing students' subjective evaluation of their knowledge before implementing this methodological approach has shown no significant difference in students' self-evaluation. The results of students' subjective understanding of cybersecurity according to gender distribution are presented in Figure 7.

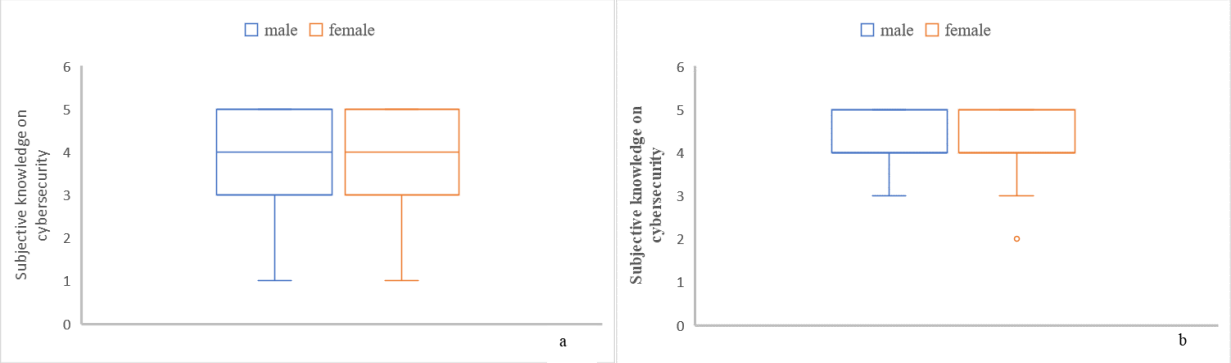

Fig. 7 Students' subjective knowledge about cybersecurity according to gender a) lower-grade b) upper-grade

Figure 7 confirms that upper-grade students have better knowledge of cybersecurity, with better distribution of their answers. On the other hand, lower-grade students' answers vary among the students. There is no gender difference in their subjective evaluations. These results are not consistent with previous studies, but they are in line with the finding from Yan et al. (2021) that gender does not influence students' cybersecurity knowledge and skills. Furthermore, the same results were obtained during the self-evaluation of the students' improvement concerning their cybersecurity knowledge and skills due to this methodological approach, which leads to the conclusion that this approach can be applied in different classes, regardless of gender.

Similar analyzes were done regarding the schools' geographical distribution to evaluate whether there is a difference in students' knowledge concerning cybersecurity between urban and rural schools. The results of this distribution are presented in Figure 8.

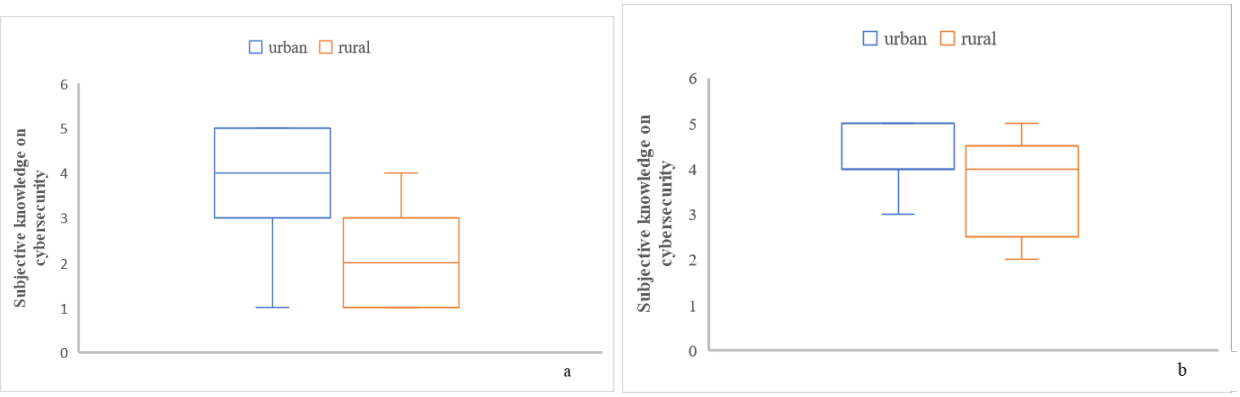

Fig. 8 Students' subjective knowledge about cybersecurity according to urbanization a) lower-grade students b) upper-grade students

The results indicate that students from rural schools have lower knowledge of cybersecurity due to students' subjective evaluation than those from urban schools. These differences are more recognizable among lower-grade students, although there are differences concerning upper-grade students, too. The mean value of lower-grade students' subjective evaluation of their knowledge concerning cybersecurity in the rural school is 2,10, in contrast to urban schools, where the mean value is 3,85. Concerning upper-grade students, the difference is not so big, so in the rural school, it is 3,60, and in urban schools, it is 4,42. These results are confirmed by a multiple-choice test carried out before the start of the implementation process. However, the number of students from the rural school that took part in this research is very small, and it cannot be used to make significant conclusions. This imbalance in the number of students from rural and urban schools is one of the limitations of our study, which need further research.

4.1. Limitations and future work

The study's design does not include a control group for comparison, which limits the ability to attribute improvements in knowledge and skills directly to the intervention. Including a control group in future research could strengthen the evidence for the effectiveness of the approach. However, given the nature of the participants, who are primary school students, implementing a control group might pose ethical and practical challenges. It is essential to consider the age and developmental stage of the participants, as exposing them to potentially beneficial interventions while withholding them from others could raise ethical concerns regarding their educational experience.

The study is conducted in a relatively homogeneous sample of schools, with relatively imbalanced data sets, especially between urban and rural participants. Expanding the sample to include a more diverse range of schools, especially increasing the representation of rural schools, could enhance the generalizability of the findings. Moreover, small sample sizes limit the reliability of more advanced statistical analyses, and uneven data distributions can lead to biased results with complex statistical methods. Therefore, we decided to use simple statistical technique (averages) to make sense of the data without risking misleading conclusions. Despite these limitations, the obtained results managed to provide insights into the benefits of the proposed methodology within the context of primary school education.

Carrying out the proposed methodology on a larger sample size could validate the findings of this study. Possible future work could refer to going even further in the methodology implementation, putting lower-grade students in the tutor role, and teaching even younger students about cybersecurity. A more detailed analysis of gender, socio-economic background, and their influence on learning outcomes could provide deeper insights into the equity of the educational approach. Addressing technological accessibility and proposing strategies for low-resource settings could enhance the approach's inclusivity.

The presented methodological approach can be easily adapted to various contexts and educational levels. The practice of informed consent provided before starting with the implementation should be continued in that case together with the consent of “older” students to share created educational resources.

The article focuses on the immediate outcomes of the implemented methodological approach without assessing its long-term impact on students' knowledge retention and behavior change. Our future work will explore the sustainability of the learning gains and the long-term effectiveness of the approach. To achieve this, we will evaluate the acquired knowledge and skills one year after the implementation of the proposed approach, and we will compare the results. Long-term impact on students’ knowledge and skills could provide a more comprehensive understanding of the approach's effectiveness.

5. Conclusion

The paper presents a novel methodological approach for learning cybersecurity topics in primary education. The proposed methodology aims to enhance students' cybersecurity competencies in an enjoyable and engaging manner. We established an interactive learning environment where students feel comfortable sharing their views and learning about internet safety. Peer-to-peer learning was used to build a community of learners. We incorporated game-based activities to achieve active involvement, engagement, and enjoyment during learning. This involved creating a cybersecurity-themed game for upper-grade students (8^{th} and 9^{th} grade) and a play-to-learn game for lower-grade students (6^{th} and 7^{th} grade).

Upper-grade students were actively involved in the learning process, where they acquired knowledge through the hands-on preparation of materials. They were considered how these materials would be shared with lower-grade students. These activities improved their cybersecurity understanding and enhanced their critical thinking, communication, and teamwork abilities.

Students’ self-evaluation of the improvement of their knowledge and skills as the result of this methodological approach indicates that all students have improved their knowledge and abilities. Upper-grade students have seen a slightly more significant improvement due to their active role in creating educational materials. This highlights the

effectiveness of learning through hands-on experience. Nevertheless, the subjective evaluation reveals that the proposed approach has also improved lower-grade students' competencies.

The study found that there was no gender difference in the students' self-evaluation of their cybersecurity knowledge before the study. Additionally, the same results were obtained when the students self-evaluated their progress in cybersecurity knowledge and skills after the study. This leads to the conclusion that this methodological approach to teaching cybersecurity can be applied in different classes, regardless of gender.

An analysis was conducted to compare the geographical distribution of schools and determine if there is a disparity in students' cybersecurity knowledge between urban and rural schools. The findings suggest that rural school students have lower cybersecurity knowledge, according to their subjective evaluation than urban school students. This difference is more pronounced among lower-grade students, although some disparities exist among upper-grade students, too. However, the small number of students from rural school participating in the study limits the ability to make definitive conclusions.

Declarations:

Funding: No funding was received to assist with the preparation of this manuscript.

Conflict of interest: The authors declare that they have no conflict of interest.

Ethic statement: All procedures performed in studies involving human participants were in accordance with the ethical standards and laws of the North Macedonia. Informed consent was obtained from all individual participants included in the study.

Data availability statement: The authors confirm that the data supporting the findings of this study are available on request from the corresponding author.

Authors' contribution statements: All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Maja Videnovik, Sonja Filiposka and Vladimir Trajkovik. The first draft of the manuscript was written by Maja Videnovik and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

References:

Ädel, E., Löfmark, A., Pålsson, Y., Mårtensson, G., Engström, M., & Lindberg, M. (2021). Health-promoting and -impeding aspects of using peer-learning during clinical practice education: A qualitative study. *Nurse Education in Practice*, *55*, 103169. https://doi.org/10.1016/j.nepr.2021.103169

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. *Future Internet*, *11*(3), Article 3. https://doi.org/10.3390/fi11030073

Amo, L. (2016). Addressing gender gaps in teens' cybersecurity engagement and self-efficacy. *IEEE Security & Privacy*, *14*(1), 72–75. https://doi.org/10.1109/MSP.2016.12

Balakrishna, C. (2021). Design considerations for developing a game-based learning resource for cyber security education. In *Proceedings of the European Conference on Games-based Learning* (pp. 80-89). https://doi.org/10.34190/ecgbl.16.1.804

Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, *27*(3), 3011–3036. https://doi.org/10.1007/s10639-021-10704-y

Cardinot, A., & Fairfield, J. A. (2019). Game-based learning to engage students with physics and astronomy using a board game. *International Journal of Game-Based Learning*, *9*(1), 42–57. https://doi.org/10.4018/IJGBL.2019010104

Chandra, S., & Palvia, S. (2021). Online education next wave: Peer to peer learning. *Journal of Information Technology Case and Application Research*, *23*(3), 157–172. https://doi.org/10.1080/15228053.2021.1980848

Chen, C. H., Liu, J. H., & Shou, W. C. (2018). How competition in a game-based science learning environment influences students' learning achievement, flow experience, and learning behavioral patterns. *Educational Technology & Society*, *21*(2), 164–176.

Chowdhury, N., & Gkioulos, V. (2023). A personalized learning theory-based cyber-security training exercise. *International Journal of Information Security*, 1-16. https://doi.org/10.1007/s10207-023-00704-z

Deshpande, P., Lee, C. B., & Ahmed, I. (2019). Evaluation of peer instruction for cybersecurity education. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (pp. 720–725). https://doi.org/10.1145/3287324.3287403

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*, *1339*(1), 012098. https://doi.org/10.1088/1742-6596/1339/1/012098

Gamlath, S. (2022). Peer learning and the undergraduate journey: A framework for student success. *Higher Education Research & Development*, *41*(3), 699–713. https://doi.org/10.1080/07294360.2021.1877625

Hafeez, M. (2021). Effects of game-based learning in comparison of traditional learning to provide effective learning environment- a comparative review. *International Journal of Social Sciences & Educational Studies*, *8*(4). https://doi.org/10.23918/ijsses.v8i4p100

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security, 95*, 101827. https://doi.org/10.1016/j.cose.2020.101827

Hussein, M. H., Ow, S. H., Cheong, L. S., & Thong, M.-K. (2019). A digital game-based learning method to improve students' critical thinking skills in elementary science. *IEEE Access*, *7*, 96309–96318. https://doi.org/10.1109/ACCESS.2019.2929089

Ion, G., Barrera-Corominas, A., & Tomàs-Folch, M. (2016). Written peer-feedback to enhance students' current and future learning. *International Journal of Educational Technology in Higher Education*, *13*(1), 15. https://doi.org/10.1186/s41239-016-0017-y

Javidi, G., & Sheybani, E. (2019). Transforming cybersecurity education through consulting. *Systemics, Cybernetics and Informatics, 17*(1), 157-168.

Kaban, A. (2021). Secure internet use in information technologies and software course textbooks at primary and secondary schools. *Athens Journal of Education*, *8*(1), 37–52. https://doi.org/10.30958/aje.8-1-3

Kam, H. J., & Katerattanakul, P. (2019). Enhancing student learning in cybersecurity education using an out-of-class learning approach. *Journal of Information Technology Education: Innovations in Practice*, *18*, 029–047. https://doi.org/10.28945/4200

Ke, F., Shute, V., Clark, K. M., & Erlebacher, G. (2019). *Interdisciplinary design of game-based learning platforms: A phenomenological examination of the integrative design of game, learning, and assessment*. Springer International Publishing. https://doi.org/10.1007/978-3-030-04339-1

Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies*, 1-25. https://doi.org/10.1007/s10639-021-10807-6

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice*, *2018*(1), 6.

Kusuma, G. P., Putera Suryapranata, L. K., Wigati, E. K., & Utomo, Y. (2021). Enhancing historical learning using role-playing game on mobile platform. *Procedia Computer Science*, *179*, 886–893. https://doi.org/10.1016/j.procs.2021.01.078

Lee, S. M. (2019). Her story or their own stories? Digital game-based learning, student creativity, and creative writing. *ReCALL*, *31*(3), 238–254. https://doi.org/10.1017/S0958344019000028

Leune, K., & Petrilli, S. J. (2017). Using Capture-the-Flag to enhance the effectiveness of cybersecurity education. In *Proceedings of the 18th Annual Conference on Information Technology Education* (pp. 47–52). https://doi.org/10.1145/3125659.3125686

Lim, C., Jalil, H. A., Ma'rof, A., & Saad, W. (2020). Peer learning, self-regulated learning and academic achievement in blended learning courses: A structural equation modeling approach. *International Journal of Emerging Technologies in Learning (IJET)*, *15*(3), 110–125. https://www.learntechlib.org/p/217022/

Marengo, A., Pagano, A., & Soomro, K. A. (2024). Serious games to assess university students' soft skills: investigating the effectiveness of a gamified assessment prototype. *Interactive Learning Environments*, 1-17. https://doi.org/10.1080/10494820.2023.2253849

Martin, F., Gezer, T., & Wang, C. (2019). Educators' perceptions of student digital citizenship practices. *Computers in the Schools*, *36*(4), 238-254. https://doi.org/10.1080/07380569.2019.1674621

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Muir, K., & Joinson, A. (2020). An exploratory study into the negotiation of cyber-security within the family home. *Frontiers in Psychology*, *11*. https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00424

Nerantzi, C. (2020). The use of peer instruction and flipped learning to support flexible blended learning during and after the COVID-19 pandemic. *International Journal of Management and Applied Research*, *7*(2), 184–195. https://www.ceeol.com/search/article-detail?id=883236

Olano, M., Sherman, A., Oliva, L., Cox, R., Firestone, D., Kubik, O., Patil, M., Seymour, J. & Thomas, D. (2014). SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68–74. https://doi.org/10.1109/MSEC.2020.2969409

Rahman, N., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cyber security in schools: The Human Factor. *Educational Planning*, *27*(2), 23-39.

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113-122). https://doi.org/10.1145/2047594.2047628

Sağlam, R. B., Miller, V., & Franqueira, V. N. L. (2023). A systematic literature review on cyber security education for children. *IEEE Transactions on Education*, 1–13. https://doi.org/10.1109/TE.2022.3231019

Sánchez-Mena, A., & Martí-Parreño, J. (2017). Teachers´ acceptance of educational video games: A comprehensive literature review. *Journal of E-Learning and Knowledge Society*, *13*(2). https://www.learntechlib.org/p/188115/

Scheider, B., & Asprion, P. M. (2023). Peer Instruction as Teaching Method in Cybersecurity and Data Privacy. *International Journal of Management, Knowledge and Learning*, *12*. https://doi.org/10.53615/2232-5697.12.1-7

Sung, H. Y., & Hwang, G.-J. (2013). A collaborative game-based learning approach to improving students' learning performance in science courses. *Computers & Education*, *63*, 43–51. https://doi.org/10.1016/j.compedu.2012.11.019

Suson, R. L. (2019). Appropriating digital citizenship in the context of basic education. *International Journal of Education, Learning and Development*, *7*(4), 44-66.

Topping, K. J. (1996). The effectiveness of peer tutoring in further and higher education: A typology and review of the literature. *Higher Education*, *32*(3), 321–345. https://doi.org/10.1007/BF00138870

Triplett, W. J. (2023). Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability*, *3*(1), 47-67. https://doi.org/10.52889/ijses.v3i1.132.

Vankúš, P. (2021). Influence of game-based learning in mathematics education on students' affective domain: A systematic review. *Mathematics*, *9*(9), Article 9. https://doi.org/10.3390/math9090986

Videnovik, M., Vold, T., Kiønig, L., & Trajkovik, V. (2019). Design thinking methodology for increasing quality of experience of augmented reality educational games. In *18th International Conference on Information Technology Based Higher Education and Training (ITHET)* (pp. 1-9). IEEE. https://doi.org/10.1109/ITHET46829.2019.8937385

Vlahu-Gjorgievska, E., Videnovik, M., & Trajkovik, V. (2018). Computational thinking and coding subject in primary schools: Methodological approach based on alternative cooperative and individual learning cycles. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)* (pp. 77–83). https://doi.org/10.1109/TALE.2018.8615334

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education*, *186*, 104536. https://doi.org/10.1016/j.compedu.2022.104536

Xiao, Y., & Lucking, R. (2008). The impact of two types of peer assessment on students' performance and satisfaction within a Wiki environment. *The Internet and Higher Education*, *11*(3), 186–193. https://doi.org/10.1016/j.iheduc.2008.06.005

Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior*, *121*, 106791. https://doi.org/10.1016/j.chb.2021.106791

Zhao, D., Muntean, C. H., Chis, A. E., & Muntean, G.-M. (2021). Learner attitude, educational background, and gender influence on knowledge gain in a serious games-enhanced programming course. *IEEE Transactions on Education*, *64*(3), 308–316. https://doi.org/10.1109/TE.2020.3044174