https://doi.org/10.53656/math2027-1-5-asi

THE PRESENCE OF INTERNET SAFETY IN THE NATIONAL CORE CURRICULUM OF SLOVAKIA FROM A CENTRAL EUROPEAN COMPARATIVE PERSPECTIVE

Bence Pásztor, Gábor Kiss
Department of Informatics, J. Selye University, Komárno (Slovakia)

Abstract. This research examines one segment of IT education. The role of internet safety education in primary and secondary school is becoming more and more important, because young people usually start using the internet at an early age for learning, entertainment, and communication. However, due to this early use, they are also more likely to encounter online dangers such as cyberbullying, online fraud, data misuse and privacy violations. The aim of the study is to map how internet safety awareness education is reflected in the state-issued curriculum in Slovakia. Furthermore, we aim to present the development opportunities and possible shortcomings by comparing it with other Central European countries. In this study we analyze the Austrian, Czech, Hungarian and Polish national core curricula in relation to the Slovak curriculum. The research is based on document analysis.

Keywords: national core curriculum; internet safety; education; Slovakia; online threats; Central Europe

1. Introduction

The rapid development of digital technology has fundamentally changed society and our everyday lives. Nowadays, children are coming into contact with internet-connected devices such as tablets, smartphones, smart TVs, and computers at an increasingly young age. This development offers many new opportunities for information gathering, learning, and entertainment, but it also poses serious challenges (Smahel et al., 2020). While in 2005 only about half of households in OECD countries had an internet connection, by 2023 this figure had risen to 92%. According to international surveys, almost

all 15-year-olds and the vast majority of 10-year-olds now live in homes with internet access. The number of people using the internet has also increased significantly: in 2005, only 30% of the population used the internet, while in 2023 this figure had risen to 80%.[1] In 2025, 6 billion people worldwide used the internet.[2] Children aged 8 – 12 spend almost six hours a day using various digital devices and content (Kumar et al., 2018). According to the 2024 DataReportal report, internet penetration in Slovakia is 91.4%, which represents more than 5.25 million users.[3] Due to the growth of online presence, the risks of the digital space and issues related to internet safety have also come to the fore; therefore, it is extremely important that students receive adequate training in data security (Quayyum & Jaccheri, 2021). Developing digital skills helps young people to navigate the online space with greater confidence, which is also useful in the labor market, as it will also be important for them to have adequate data security knowledge later on in the world of work (Luić & Švelec-Juričić & Mišević, 2021; Laybats & Tredinnick, 2016).

It is crucial that the national core curriculum also adequately addresses this topic so that schools can more effectively prepare students to deal with data security challenges (Ondrušková & Pospíšil, 2023). Technological advances and the rapidly changing dangers associated with the online space make the work of both educators and education policy leaders difficult. Although children under the age of 12 are increasingly active users of online platforms, little research has been done on how these children can acquire knowledge and coping strategies related to online data protection (Desimpelaere & Hudders & Van de Sompel, 2020). Based on previous international literature, it can be said that children in Scotland have insufficient knowledge of cyber security, and Scottish education policy and curriculum are not keeping pace with technological developments and children's early use of devices. The curriculum addresses online risks, such as phishing and hacking, too late; does not set appropriate expectations in terms of age; and does not define measurable requirements (Lamond et al., 2022). In American public education, school administrators, IT specialists, and teachers do not have sufficient resources and knowledge to deal with data protection and internet safety issues related to digital devices in schools

(Chanenson et al., 2023); therefore, increasing the awareness of internet safety among teacher training students should be considered a high priority in their education (Kiss, 2019). The EU introduced the NIS Directive in response to cyber threats in order to strengthen the security of network and information systems. The enhanced NIS2 Directive sets stricter security and incident reporting requirements (Min & Chai & Han, 2015; Ristvej et al., 2025).

This study aims to map how internet safety awareness education is reflected in the state-issued curriculum in Slovakia. Furthermore, we examine the national core curricula of four European countries in comparison with the Slovak national core curriculum: Austria, Poland, Hungary, and the Czech Republic with the aim of identifying opportunities for further development and the possible shortcomings.

2. Methodology of the research

The aim of the research is to explore the extent to which internet safety education is included in the national core curriculum for primary and secondary schools in Slovakia. A key element of the research is to compare the Slovak national core curriculum with the national core curricula of other Central European countries (Austria, Hungary, Poland, and the Czech Republic) to identify opportunities for its expansion so that students are exposed to the topic of internet safety as early as possible. We determined which country's curricula covered the most of the internet safety subtopics and knowledge areas at each school level. This approach made it possible to highlight examples of good practice and potential opportunities for expanding the Slovak curriculum in order to introduce internet safety education to students as early and comprehensively as possible. The research therefore maps out what internet safety knowledge students should acquire at what age according to the national core curriculum.

The research has shown that the countries studied use different terms to refer to IT education. In Austria, students are first introduced to IT in Digital literacy classes and then continue their studies in Computer science classes. In Hungary the name of the course is Digital culture, while in Slovakia, Poland and Czech Republic students learn IT in Informatics lessons. Hereinafter, these will be collectively referred to as IT classes.

This research employs qualitative document analysis. During the study, we analyzed the framework curriculum documents for IT subjects, paying particular attention to the extent to which internet safety is covered. In particular, the analysis focused on the scope and depth of internet safety education, the number of internet safety-related subtopics included, the age or educational stage at which these topics are introduced, and the continuity of their development across different educational levels. We compiled all the topics related to internet safety from the official national core curriculum guidelines. We organized these topics into tables by school level to examine which countries cover internet safety in depth, which topics are included in the curriculum of every country we examined, and which topics are addressed by only a few countries. Based on our tables, we also observed whether there are topics that appear at different school levels but are present in multiple countries. Following a review of the core curricula, we then outlined potential areas for development for Slovakia.

The study relies exclusively on national core curriculum documents for primary and secondary schools and did not include the curricula of other types of schools. We did not examine vocational secondary schools because they have an extremely variable structure. For instance, in Slovakia, there are numerous specializations, each of which includes several different subjects. These subjects would need to be examined separately in order to obtain meaningful, comparable results. The vocational training structure is constantly changing from year to year to meet the needs of the labor market. As a result, by the time a comprehensive analysis was completed, some of the data and categories examined would already be outdated, so the research would have to be restarted from scratch. Due to these factors, the inclusion of vocational secondary schools in the present study would not have been methodologically sound or effective. The data required for the analysis were collected electronically from reliable, official sources.

3. School system and number of IT classes in the Central European countries studied

A common feature of the education systems in the Central European countries examined is that they all have an official curriculum issued at the state level. This document sets out the basic content and requirements that

public education institutions in the country must follow. The framework curriculum ensures a uniform standard of education in each country, while at the same time giving schools the freedom to adapt their teaching methods and supplementary content to local needs, conditions, and profiles in their own pedagogical programs and local curricula.[4,5,6,7,8,9,10,11]

Table 1. The number of IT lessons based on the curricula[4,5,6,7,8,9,10,11]

Country	**Education level and grades**		**Ages of the students**	**Number of IT lessons (summarized for the given level of education)**
Austria	primary school	grades 1–4	6–10	no IT lessons
	secondary school	lower secondary level (grades 5–8)	10–14	4 lessons (1-1-1-1)
		upper secondary level(grades 9–13)	14–18	2 lessons (2-0-0-0)
Hungary	basic school	grades 1–4	6–10	2 lessons (0-0-1-1)
		grades 5–8	10–14	4 lessons (1-1-1-1)
	upper secondary grammar school	grades 9–12	14–17	5 lessons (2-1-2-0)
Slovakia	primary education	primary education (grades 1–4)	6–10	2 lessons (0-0-1-1)
		lower secondary education (grades 5–8)	10–15	4 lessons (1-1-1-1-0)
	secondary school	upper secondary education (grades 1–4)	15–18	3 lessons (1-1-1-0)
Czech Republic	basic education	primary education (grades 1–5)	6–11	2 lessons (0-0-0-1-1)
		lower secondary education (grades 6–9)	11–15	4 lessons (1-1-1-1)

	secondary school	upper secondary education (grades 1–4)	15–18	4 lessons
Poland	primary school	early school education (grades 1–3)	7–10	at school's discretion
		teaching by subject (grades 4–8)	10–15	5 lessons (1-1-1-1-1)
	general secondary school	grades 1–4	15–18	3 lessons (1-1-1-0)

In Poland, the national core curriculum for early school education only stipulates that computer science must be taught at that level, but the number of lessons is left to the school's discretion. In Austria, primary school pupils may encounter IT knowledge as part of other subjects, such as German, German as a second language, mathematics, art and technology, and design. Based on Table 1, it can be said that Slovakia ranks in the middle in terms of the number of lessons determined by the national core curriculum, as both Hungary and the Czech Republic have more IT lessons for students until the end of secondary education, even though Hungarian public education is shorter, as students attend school for 12 years until the end of upper secondary education, while in Slovakia they attend school for 13 years. Poland is the only country where students have five IT lessons in lower secondary school level, which is referred to in Poland as "subject teaching" (nauczanie przedmiotowe). Hungary has the highest number of IT lessons at the secondary school level. Based on this, it is clear that Slovakia could increase the number of IT lessons in elementary school and secondary school, as Slovakia has 4 IT lessons in lower secondary school and 3 IT lessons in upper secondary school, according to the national core curriculum.

The figures in parentheses in the last column of Table 1 indicate the number of weekly IT class lessons in each grade in different countries. Based on this, it can be said that in most grades, students attend one IT lesson per week. There are only three exceptions to this rule, in which students have two lessons of IT class per week: first grade of upper secondary level

in Austria, and 9 and 11 grades of upper secondary grammar school education in Hungary.

4. Internet safety education based on the national core curriculum for Informatics in Slovakia

In Slovakia, performance and content standards are linked to each topic in the Informatics curriculum. The performance standard defines the knowledge and skills that students must acquire, while the content standard defines the teaching material through which they can achieve this. "Safety and Risks" is covered four times in Slovakia's national core curriculum: once in primary education, twice in lower secondary education, and once in secondary school. [12,13,14]

4.1. Internet safety education at primary school level

The performance standard stipulates that by the end of the 4th grade of primary school, pupils should be able to identify the dangers of the internet and understand how to prevent illegal use of email. Complementing this, the content standard dictates that children must understand the principles of safe online behavior.[12]

The lower secondary school curriculum addresses "Safety and risks" twice. Based on performance standards, by the end of 6th grade, students should be familiar with various online risks and know how to protect applications, data and email from unauthorized access. Students should also be able to evaluate the accuracy of material provided online and talk about cybercrime. The corresponding content standard covers malicious software (such as viruses), the reliability of retrieved information, the dangers of social networking sites, the dissemination of malware and spam, safe and ethical online conduct, and hacker activities.

By the end of the 8th grade, performance criteria require pupils to analyze internet-related dangers. They must be able to determine which types of data require protection against theft, implement regulations to prevent unlawful computer use, and secure social media and email accounts. Additionally, students are required to recognize the threats posed by malicious software, assess the reliability of online content, and explain concepts related to cybercrime, computer crime, and the risks of illicit content. At this stage, the content standard details viruses as malicious

software (malware), spam messages, and the deployment of antivirus software for system protection. It also emphasizes the significance of strong passwords as a fundamental security component, alongside the challenges surrounding data accuracy on the internet and social media platforms. Safe and ethical online conduct, hacker activities, and protection against computer infections are central to the topics covered.[13]

4.2. Internet safety education at secondary school level

The topic of "Safety and risk" also appears in the Informatics curriculum for upper secondary education. The performance standard states that pupils have to be able to evaluate the dangers associated with using malware. To prevent illegal use, students also need to be aware of the guidelines for secure connection to computers, websites for social networking, and emails. Students must be able to evaluate the accuracy of information available on websites and make sure that data and communications are safeguarded against misuse. They must be able to identify illegal content and recognize crimes. The content standard goes into great detail about how viruses and spam spread, the fundamentals of ethical and safe online conduct, the actions of hackers, and ways to prevent sharing personal information online.[14]

5. The emergence of internet safety education in the national core curricula of other Central European countries

5.1. Internet safety at the lowest level of public education in Central European countries

In Table 2, we examine the content regarding the topic internet safety appearing at the lowest level of education in order to observe international best practices that may be re-evaluated in terms of the Slovak curriculum:

Based on the official, national core curriculum, Hungary is following a strategy of introducing students to basic internet safety skills in more detail as early as the grades 3 and 4 of basic schools. Consequently, Hungary stands out in preparing its youngest children to recognize online dangers. The curriculum also addresses the ethics of using mobile phones alongside computers. This reflects how the National Core Curriculum (which entered into force in 2020) adapted to the growing trend of mobile phone adoption among increasingly younger children. It is also worth highlighting the

Hungarian best practice of not only teaching children in this age group theoretical knowledge about internet safety but also applying a practical approach, for example, through role-playing games. This greatly contributes to students gaining experience and being able to handle real-life situations more easily. In contrast, as we saw in the previous chapter, the topic is only touched upon in Slovakia's primary school curriculum. Based on the example of Hungary, Slovakian students' knowledge of internet safety could also be expanded, which would be relevant given children's leisure habits. In particular, the ethics of mobile device use, online harassment, and internet addiction management would be important to incorporate into the Slovak curriculum, as the surveys described earlier show that children spend a lot of time on computers and in the online world.

Table 2. Internet safety education at the lowest level of public education in Central European countries based on the national core curriculum[15,5,16,10]

Country	Grades	Internet safety content
Hungary	basic school grades 1–4	Recognizing the dangers of the internet Protecting personal data Recognizing fake news Dealing with online harassment and internet addiction Passwords and secure communication Ethics of using mobile devices Exercises: role-playing, reasoning, counselling
Austria	primary school grades 1–4	no specific guidelines, no independent IT education
Czech Republic	basic education grades 1–5	Understanding user accounts and passwords Introduction to basic data protection concepts (with limited detail)
Poland	primary school grades 1–3	no central guidelines

5.2. The emergence of internet safety in middle-level public education in Central European countries

In Slovak and Austrian lower secondary schools, the curricula prescribe more in-depth content, such as secure password use, assessing the credibility of information, and protection against malicious programs.

Table 3. Internet safety at the middle-level of public education in Central European countries based on the national core curriculum[5,10,16,17]

Country	Grades	Internet safety content
Hungary	primary school grades 5–8	internet safety is not mentioned at this level
Austria	lower secondary school levels grades 1–4	Grade 1: simple internet searches and checking the quality of the found information; use and protection of data and personal data; collection, storage, and use of user data Grade 2: providing and retrieving information; data transfer; licensing models Grade 3: media usage habits, opportunities and risks of media usage; risks related to digital technologies; responsible handling of information and data, critical evaluation of found information; operation of cloud-based systems; data security and data protection; protection of digital identity; application of encryption methods; secure password use and two-factor authentication; digital protection of electronic information; cybersecurity (cyberbullying, cyber grooming, identity theft); protection against viruses and malware Grade 4: the possibilities and limitations of artificial intelligence; data backup and recovery; the risks of collecting, analyzing, and linking user data; mechanisms for constructing media reality; image, sound, and data manipulation; responsible communication and data exchange; copyright and the right to self-image; the phenomenon of viral content spread and related courses of action; knowledge of data protection legal bases (GDPR)
Czech Republic	basic education grades 6–9	Minimizing the risk of loss or misuse of data Unreliable applications and systems Security of digital devices and data – updates, antivirus software, firewalls Secure password management and password managers, two-step authentication, data and communication encryption Data backup and archiving
Poland	primary school grades 4–8	Grades 4–6: data protection, intellectual property rights, information-related risks and protection Grades 7–8: security, protection of digital identity and privacy, intellectual property rights, and equal access to information

At the same time, the Austrian curriculum takes a more detailed approach at this stage, with a stronger emphasis on cyberbullying, cyber

grooming, identity theft, and the management and protection of user data. This level of detail suggests that Austria is consciously responding to the new risks of the information society. It is worth highlighting the element of the Austrian curriculum that requires reflection on the possibilities and limitations of artificial intelligence, as well as practice in data backup and recovery. In addition, there is a strong emphasis on developing media literacy, including understanding the construction of media reality, recognizing data and media manipulation, and discussing various licenses and the GDPR in detail. These elements show that the Austrian framework curriculum integrates new technological and social challenges more effectively, particularly in the areas of data protection and artificial intelligence. Adapting to technological shifts is crucial for the Slovak national curriculum. Rapid advancements, particularly the spread of artificial intelligence, introduce new ethical and safety challenges currently unaddressed by the existing framework.

5.3. The emergence of internet safety at secondary school level

Table 4 summarizes the internet safety-related content of national core curricula for secondary schools (in Austria, upper secondary school level).

At the general secondary school level, Poland deals with the issue of internet safety in the most detail. At this level, too, the Polish national curriculum deals extensively with issues such as respect for intellectual property. Students not only learn basic security concepts but also gain practical knowledge about data protection, ethical internet use, legal frameworks (e.g., copyright, data protection), and the recognition and management of digital threats such as viruses, spam, and hacking. Poland places particular emphasis on the importance of encryption and authentication, as well as electronic signatures.

The Slovak national core curriculum does not add any new perspectives to what has been learned so far, so students at this level repeat the information they have already learned and expand their knowledge in this area. However, although the Slovak national core curriculum is the most detailed after the Polish one in terms of internet safety education at secondary school level, it would be important to cover new topics in addition to deepening existing knowledge, as in the Polish core curriculum.

Table 4. The topic of internet safety at the secondary school level in Central European countries based on the national core curriculum[18,11,6,9]

Country	Grades	Internet safety content
Hungary	upper secondary grammar school grades 1–4	Defence against various forms of online harassment and requesting help when necessary
Austria	upper secondary school levels grades 5–8	Knowledge and application of measures and legal principles relating to data security, data protection, and copyright
Czech Republic	secondary school grades 1–4	the topic of internet safety is not mentioned at this level
Poland	general secondary school grades 1–4	Respect for privacy, data protection, and intellectual property Application of communication netiquette Recognition and management of technological risks Compliance with legislation (data protection, copyright) Following ethical standards when using digital content Practices for protecting sensitive data (e.g., passwords, PIN codes) Data security and operating system protection The role of encryption and authentication in information protection Recognizing the negative effects of piracy The importance of electronic signatures and encryption procedures

Nowadays, forms of digital administration that require electronic signatures or authentication are becoming increasingly common, so it is important that students are also aware of the risks associated with them. At the secondary school level, students' activities are already extremely diverse, characterized by social media platforms, dating sites, email accounts, and visiting websites, all of which can pose a wide variety of risks. It is therefore important that students expand their knowledge at this level and learn about issues that will help them deal with real-life online dangers. In addition, although none of the curricula examined specifically address this issue, in line with modern practices, it would be important for students to acquire internet safety knowledge related to online banking and payments at least at this age.

6. Conclusion

This study examined how internet safety appears in the Slovak national core curriculum from primary to secondary school level and compared Slovak educational policy regarding the teaching of internet safety with the curricula of Austria, the Czech Republic, Poland, and Hungary. The findings show that internet safety is already present in Slovak education from an early age and follows a gradual, age-appropriate structure. However, the comparative analysis also revealed several areas in which the Slovak curriculum could be expanded and updated.

The reviewed international examples highlight the importance of addressing emerging digital risks and students' everyday online activities in greater depth. Topics such as online harassment, internet addiction, fake news, artificial intelligence, data protection, encryption, authentication, and electronic signatures are treated more comprehensively in several neighboring countries and could strengthen internet safety education in Slovakia as well. Given the rapid technological development and the increasing early use of digital devices by children, curricula must remain flexible and responsive to new online challenges.

The study is limited by the different school systems and by its focus on national core curricula. The study does not evaluate how internet safety is implemented in classroom practice or how effectively students acquire related competencies. Future research should therefore include empirical investigations involving students and teachers in order to assess actual levels of internet safety awareness and educational outcomes.

Overall, the findings suggest that while the Slovak curriculum provides a solid foundation for internet safety education, further modernization and expansion of the curriculum would better prepare students for the digital challenges of contemporary society.

NOTES

1. Organisation for Economic Co-operation and Development. How's Life for Children in the Digital Age? Revised version, June 2025. Paris: OECD Publishing. https://doi.org/10.1787/0854b900-en

2. Statista. Number of internet users worldwide from 2005 to 2024. https://www.statista.com/statistics/617136/digital-population-worldwide/
3. DataReportal. Digital 2024: Slovakia. Kepios / We Are Social / Meltwater. https://datareportal.com/reports/digital-2024-slovakia
4. Hungarian Official Gazette. Table II.2.1.3 (in Hungarian: Magyar Közlöny, II.2.1.3. táblázat)
5. https://magyarkozlony.hu/dokumentumok/3288b6548a740b9c8daf918a399a0bed1985db0f/megtekintes
6. Ministry of Education, Youth and Sports of the Czech Republic. Framework Educational Programme for Basic Education (in Czech: Ministerstvo školství, mládeže a tělovýchovy, Rámcový vzdělávací program pro základní vzdělávání). https://www.edu.cz/wp-content/uploads/2023/07/RVP_ZV_2023_cista_verze.pdf
7. Ministry of Education, Youth and Sports of the Czech Republic. Framework Educational Programme for Secondary Schools (in Czech: Ministerstvo školství, mládeže a tělovýchovy, Rámcový vzdělávací program pro gymnázia). https://www.edu.cz/wp-content/uploads/2020/08/RVPG-2007-07_final.pdf
8. Ministry of Education, Research, Development and Youth of the Slovak Republic. State Educational Programme (in Slovak: Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky, Štátny vzdelávací program). https://www.minedu.sk/data/att/473/22021.94bec0.pdf
9. National Institute for Education and Youth. Innovated State Educational Programme – Curriculum for Secondary Schools (in Slovak: Národný inštitút vzdelávania a mládeže, Inovovaný štátny vzdelávací program – rámcový učebný plán pre gymnáziá). https://www.statpedu.sk/files/articles/dokumenty/inovovany-statny-vzdelavaci-program/rup_g_4_r_s_vyuc_jaz_slov.pdf
10. Sejm of the Republic of Poland. Act of 24 May 2024 (in Polish: Sejm Rzeczpospolitej Polskiej, Ustawa z dnia 24 maja 2024 r.).

https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20240000781/O/D20240781.pdf

11. Federal Chancellery of the Republic of Austria. Primary School Curriculum – Annex 1 (in German: Bundeskanzleramt der Republik Österreich, Lehrplan der Volksschule, Anl. 1). https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009275&Anlage=1
12. Federal Chancellery of the Republic of Austria. Curricula for Academic Secondary Schools – Annex 1 (in German: Bundeskanzleramt der Republik Österreich, Lehrpläne – allgemeinbildende höhere Schulen, Anl. 1). https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008568&Anlage=1
13. Ministry of Education, Research, Development and Youth of the Slovak Republic. Informatics – Primary Education (in Slovak: Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky, Informatika – primárne vzdelávanie). https://www.minedu.sk/data/att/542/22036.5e0a91.pdf
14. Ministry of Education, Research, Development and Youth of the Slovak Republic. Informatics – Lower Secondary Education (in Slovak: Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky, Informatika – nižšie stredné vzdelávanie). https://www.minedu.sk/data/att/2d2/22091.7fd543.pdf
15. National Institute for Education and Youth. Informatics – Secondary School Programme (Four- and Five-year Programmes) (in Slovak: Národný inštitút vzdelávania a mládeže, Informatika – gymnázium so štvorročným a päťročným vzdelávacím programom). https://www.statpedu.sk/files/articles/dokumenty/inovovany-statny-vzdelavaci-program/informatika_g_4_5_r.pdf
16. Hungarian Educational Authority. Digital Culture Curriculum Framework for Grades 3–4 (in Hungarian: Oktatási Hivatal, Digitális

kultúra kerettanterv 3–4 évfolyam). https://www.oktatas.hu /pub_bin/dload/kozoktatas/kerettanterv/Digitalis_kultura_A.docx
17. Ministry of Education of Poland. Core Curriculum for Grades I – III of Primary School (in Polish: Ministerstwo Edukacji, Podstawa programowa dla klas I – III szkoły podstawowej). https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20240000996/O/D20240996.pdf
18. Hungarian Educational Authority. Digital Culture Curriculum Framework for Grades 5–8 (in Hungarian: Oktatási Hivatal, Digitális kultúra kerettanterv 5–8. évfolyam). https://www.oktatas.hu /pub_bin/dload/kozoktatas/kerettanterv/Digitalis_kultura_F.docx
19. Hungarian Educational Authority. Digital Culture Curriculum Framework for Grades 9–11 (in Hungarian: Oktatási Hivatal, Digitális kultúra kerettanterv 9–11 évfolyam). https://www.oktatas.hu/pub_bin/dload/kozoktatas/kerettanterv/Digitalis_kultura_K.docx

REFERENCES

Chanenson, J., Sloane, B., Morrill, A., Chee, J., Rajan, N., Huang, D. Y. & Chetty, M. (2023). Uncovering Privacy and Security Challenges in K-12 Schools. In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI 2023)* https://doi.org/10.1145/3544548.3580777

Desimpelaere, L., Hudders, L. & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, 110, 106382. https://doi.org/10.1016/j.chb.2020.106382

Kiss, G. (2019). The information security awareness of the Slovakian kindergarten teacher students at starting and finishing the study in higher education. In: *ERPA International Congresses on Education 2019 (ERPA 2019). SHS Web of Conferences*, *66*, 01042. https://doi.org/10.1051/shsconf/20196601042

Kumar, P., Vitak, J., Chetty, M., Clegg, T. L., Yang, J., McNally, B. & Bonsignore, E. (2018). Co-Designing Online Privacy-Related Games and Stories with Children. In: *Proceedings of the 2018 ACM Conference on Interaction Design and Children (IDC 2018)*, 67 – 79. https://doi.org/10.1145/3202185.3202735

Lamond, M. L., Renaud, K. V., Wood, L. A. & Prior, S. (2022). SoK: Young Children's Cybersecurity Knowledge, Skills & Practice: A Systematic Literature Review. In: *Proceedings of the 2022 European Symposium on Usable Security (EuroUSEC 2022)*, 14 – 27. https://doi.org/10.1145/3549015.3554207

Laybats, C. & Tredinnick, L. (2016). Information security. *Business Information Review*, 33(2), 76 – 80. https://doi.org/10.1177/0266382116653061

Luić, L., Švelec-Juričić, D. & Mišević, P. (2021). The Impact of Knowledge of the Issue of Identification and Authentication on the Information Security of Adolescents in the Virtual Space. *WSEAS Transactions on Systems and Control*, (16), 527 – 533. https://doi.org/10.37394/23203.2021.16.49

Min, K.-S., Chai, S.-W. & Han, M. (2015). An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications*, *9*(2), 13 – 19. https://doi.org/10.14257/ijsia.2015.9.2.02

Ondrušková, D. & Pospíšil, R. (2023). The good practices for implementation of cyber security education for school children. *Contemporary Educational Technology*, *15*(3), ep435.

Quayyum, F., Cruzes, D. S. & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Ristvej, J., Tonhauser, M., Chovanec, D., Kubás, J., Kollár, B. & Zamiar, Z. (2025). Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. *Scientific Reports*, 15, 26902. https://doi.org/10.1038/s41598-025-12829-3

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S. & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. *EU Kids Online.* https://doi.org/10.21953/lse.47fdeqj01ofo

✉ Bence Pásztor
ORCID iD: 0009-0007-2760-7012
Department of Informatics
J. Selye University
Komárno, Slovakia
E-mail: pasztor.bence@student.ujs.sk

✉ Gábor Kiss
ORCID iD: 0000-0002-0447-9376
Department of Informatics
J. Selye University
Komárno, Slovakia
E-mail: kissga@ujs.sk