Teachers' Awareness of Online Threats and Interest in Education

Jana Uramová
Department of Information Networks
Faculty of Management Science and Informatics
University of Žilina
Žilina, Slovakia
Jana.Uramova@fri.uniza.sk

Matej *Režný*
Department of Information Networks
Faculty of Management Science and Informatics
University of Žilina
Žilina, Slovakia
Matej.Rezny@stud.uniza.sk

Ondrej Škvarek
Department of Information Networks
Faculty of Management Science and Informatics
University of Žilina
Žilina, Slovakia
Ondrej.Skvarek@fri.uniza.sk

2025 International Conference on Emerging eLearning Technologies and Applications (ICETA) | 979-8-3315-7426-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICETA67772.2025.11280106

Abstract*— The study addresses the level of cybersecurity awareness among primary and secondary school teachers and their preparedness to respond to the challenges of the digital environment. The research was conducted through a questionnaire survey involving teachers from various regions of Slovakia and supplemented with qualitative reflections from respondents. The analysis revealed that most educators possess only basic knowledge, and systematic training in this area remains insufficiently widespread. Respondents expressed strong interest in practice-oriented training, particularly in relation to the prevention of cyberbullying and the protection of personal data. The findings highlight the need for developing methodological support and implementing regular training programs that reflect the specificities of the school environment and foster the digital literacy of both teachers and students.

Keywords— cybersecurity; digital literacy; cyberbullying; security awareness; teacher education

I. Introduction

In the digital age, which fundamentally transforms communication, education, and everyday life, the issue of cybersecurity and information security has become an integral part of the responsible functioning of educational institutions. Schools, as the foundational pillars in shaping the personalities of young people, face new challenges related to the safe use of technologies, the protection of personal data, the prevention of cyberbullying, and the development of digital literacy. Teachers play a key role—not only as professional guarantors of education but also as role models whose behavior can positively influence students' attitudes toward safety in the online environment.

As part of the activities of the Cybersecurity Competence Centre at the University of Žilina (UNIZA) [1], a survey was conducted in April 2025 aimed at assessing the level of awareness among primary and secondary school teachers about online threats, their experiences with cyberbullying, and their interest in further education in the field of cybersecurity. The goal of the research was to identify the current needs of teaching staff, map their attitudes toward security issues, and obtain a basis for creating effective educational programs and materials that could be developed and implemented at the level of schools, regions, or the state.

The questionnaire was designed to provide a comprehensive overview of the situation in the school environment. It contained closed questions with the possibility of adding open responses, thus ensuring higher quality and variability of the collected data. Respondents were able to express their opinions, identify shortcomings in the field of cybersecurity, and propose measures that, in their view, could contribute to increasing the safety of both students and teachers in the online environment. The research focused not only on the technical aspects of security but also on the psychological and social factors influencing students' behaviour in the digital world.

A total of 184 teachers from various types of schools and regions of Slovakia participated in the survey. Their responses represent a valuable source of information for school management, school founders, and policymakers at the national level. The analysis results may serve as a basis for strategic decision-making, the development of methodological guidelines, the updating of school curricula, and the enhancement of teachers' professional competences in digital security.

The collected data also highlight the need for systematic and regular training of teaching staff in the field of cybersecurity, as well as the importance of creating a safe digital environment for students.

II. Related works

The issue of cybersecurity and the enhancement of security awareness have been extensively studied both domestically and internationally. In recent years, the number of studies focusing on effective forms of education, the development of digital competences, and the prevention of cyber threats has been steadily increasing. [2]

A. Topics of Cybersecurity

In the professional literature, key areas have been identified that have a significant impact on the level of security awareness. These areas are described in more detail in source [2] and include:

- Cybersecurity in general
- Awareness
- Behaviour
- Internet usage and presence
- Ethics
- Privacy
- Cyberbullying

These areas form the framework within which current research operates and represent the fundamental pillars for developing educational programs focused on cybersecurity.

B. Methods of Raising Awareness

Various countries and research teams have tested several approaches that have proven to be effective in increasing users' security awareness.

1) Gamification

Authorized licensed use limited to: University of Zilina. Downloaded on September 22,2025 at 10:42:22 UTC from IEEE Xplore. Restrictions apply.

This method uses game elements for educational purposes and makes the topic more engaging. A notable example is the NoPhish application, which has been shown to significantly improve users' ability to recognize phishing attacks. [3]

2) Online educational modules

Interactive approaches play a key role in raising awareness of cybersecurity. Study [4] confirms that online modules are an effective tool for developing security habits and knowledge in the field of cybersecurity.

3) Questionnaires

Questionnaire surveys in the field of cybersecurity are used not only to assess the level of users' knowledge and attitudes, but also as part of evaluating the effectiveness of educational programs. [4]

III. Methodology and Research Methods

The research methodology was designed to provide a comprehensive view of teachers' awareness of cybersecurity issues while also enabling the formulation of practical recommendations. Within the methodology, we defined the following objectives.

A. Objectives of the Methodology

- To examine available sources and approaches to increasing security awareness.
- To create an overview of the main areas most relevant to cybersecurity in the school environment.
- To practically present the topic of cybersecurity in the school context and verify the suitability of the content for the target group.
- To conduct a questionnaire survey among primary and secondary school teachers to obtain empirical data about their knowledge, experiences, and needs in the field of digital security.

B. Review of Sources

The first step of the methodology was to conduct a review of domestic and international sources focused on increasing security awareness. The aim was to establish a theoretical foundation, identify proven methods (e.g., gamification, online modules, training programs), and compare approaches across different countries. This part also served as a basis for formulating research hypotheses and designing the questionnaire.

C. Overview of Key Areas of Security Awareness

Based on the reviewed sources, we created a visual and content overview of the key areas of security awareness. This overview served as a reference framework for the subsequent data analysis and was also used in the development of educational activities.

D. Presentation of the Topic of Cybersecurity

As part of the methodology, the issue was also practically presented during the Open Day at the UNIZA. The presentation was primarily intended for high school students, who made up the main part of the audience.

The aim of this activity was not only to popularize the topic of cybersecurity but also to practically verify which topics are most attractive to young people, what they understand, and in which areas they have the greatest shortcomings. The insights gained provided a valuable source of information that can be shared with teachers as recommendations for more effective teaching and prevention.

Interactive elements were used in the presentation (quizzes, practical demonstrations of phishing attacks, and examples of security habits), which allowed for a better understanding of students' reactions. The experiences obtained in this way contributed to complementing the results of the questionnaire survey and provided a more comprehensive picture of the state of security awareness in the school environment.

E. Questionnaire Survey

The main research method was a questionnaire survey focused on primary and secondary school teachers. A total of 184 respondents from all regions of the Slovak Republic participated in the survey. The questionnaire included both closed and open-ended questions, which were structured into four areas as outlined in the introduction. Most respondents were secondary school teachers (87%), while 13% were primary school teachers, which significantly influenced the interpretation of the results.

The questionnaire contained both closed and open-ended questions. Some questions were designed with the option of multiple responses. In the tables, these questions are marked with the note [multi-choice].

IV. Research Results

A. Respondent Characteristics

Respondents were employed at primary schools, secondary vocational schools, and grammar schools. The sample was distributed across all regions of Slovakia, with the highest representation from the Žilina region. Teachers had varying lengths of teaching practice—from beginners (less than two years) to educators with more than 20 years of experience. The sample included teachers of both general education and specialized subjects, which made it possible to compare experiences across different groups.

B. Level of Knowledge and Security Habits

The first question focused on the self-assessment of teachers' awareness of cybersecurity. The results indicate that most respondents perceive their knowledge as basic or insufficient (65%). Only one-third of teachers reported having good knowledge (34%), which suggests the need for systematic education in this area. A small proportion of respondents stated that they do not engage with this topic at all (1%). This situation may affect teachers' ability to respond effectively to cyber threats in the school environment and may also limit their capacity to educate students about safe behavior in the online world.

The second question examined teachers' personal habits when using the internet outside the school environment. The results suggest that most respondents are aware of the basic principles of personal security, such as not sharing sensitive data (91%). However, the relatively lower percentage of teachers using more advanced measures, such as two-factor authentication (42%), highlights the need to raise awareness of modern security practices. Responses within the "other" option (2%) also show that some teachers have adopted

Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:42:22 UTC from IEEE Xplore. Restrictions apply.

advanced protection techniques, which may serve as a positive example for others.

The third question focused on teachers' workplace practices when using digital technologies in the school environment. The results show that most respondents recognize the importance of protecting sensitive data (89%) and implement basic measures to secure their working environment (64%). Nevertheless, a smaller group of teachers reported not using any specific measures (6%), which points to the need to increase awareness of the risks associated with insufficient data protection in schools.

TABLE I. Teachers' Level of Knowledge and Security Habits

Q1: Do you consider yourself sufficiently informed about cybersecurity?	
Good	34%
Basic	56%
Low	9%
None	1%
Q2 *[multi-choice]*: Which security measures do you follow when using the internet and online services in your free time? online	
Strong and unique passwords for different services	65%
Regular software and operating system updates	53%
I do not share sensitive personal information	91%
I verify the legitimacy of emails	52%
Two-factor authentication	42%
I do not connect to unknown Wi-Fi networks	58%
I do not pay attention to cybersecurity	3%
Other	2%
Q3 *[multi-choice]*: Which security measures do you follow when working with computers and technologies at your school as an employee?	
Strong password for the work account	64%
I lock my Personal Computer (PC) before leaving	64%
Use the freeze function during presentations	30%
I do not leave sensitive documents and data unattended	89%
I do not use the school PC for private purposes	47%
I do not use any security measures	6%
Other	1%

C. Training and Education in the Field of Cybersecurity

The aim of the fourth question in this section was to determine teachers' actual access to professional training in the field of cybersecurity. The results indicate that cybersecurity training is not a common part of teachers' professional development. A significant proportion of respondents have never attended such training, although 40% expressed an interest in doing so. This finding highlights the need to systematically integrate cybersecurity training into school development plans, with support from school authorities and governmental bodies.

The fifth question focused on identifying specific areas of interest within potential cybersecurity training. A total of 178 teachers responded to this question. The highest level of interest was recorded in the topic of cyberbullying (75%), reflecting the relevance of this issue in the school environment. Teachers also showed interest in practical topics applicable in everyday teaching practice. The results suggest the necessity of creating training programs that respond to the real needs of teachers and combine theoretical knowledge with practical guidelines and examples.

The ninth question aimed to identify factors that would motivate teachers to participate in cybersecurity training. The findings show that teachers prefer practically oriented training—with emphasis on real-life scenarios (63%), personal online safety (61%), and the ability to serve as role models for students (51%). Interest in certification or formal recognition was much lower (19%), indicating that teachers' motivation is driven more by content and applicability than by formal acknowledgment. These insights are important for designing training programs that should be interactive, applicable, and aligned with the everyday needs of teaching practice.

The tenth question examined teachers' attitudes toward mandatory cybersecurity training. The results clearly demonstrate that most respondents view such training as important—either as a compulsory requirement (58%) or as a voluntary opportunity for professional development (40%). This consensus suggests that teachers recognize the significance of cybersecurity in their professional context and are open to systematic training as part of standard professional growth.

TABLE II. Teachers' Training in Cybersecurity

Q4: Have you ever attended cybersecurity training?	
We have regular training sessions at school	30%
On my own initiative	23%
Never, but I would like to attend such training	40%
No, I'm not interested	7%
Q5 *[multi-choice]*: If you had the opportunity to participate in cybersecurity training, which topics would interest you the most?	
How to protect personal data and passwords	42%
How to recognize fraudulent emails and websites	60%
How to prevent cyberbullying among students	75%
What types of online attacks exist and how to protect against them	65%
I don't see the need for such training	3%
Other	2%
Q9 *[multi-choice]*: What would motivate you to participate in cybersecurity training?	
Improving my personal online security	61%
Being a better role model for my students or children	51%
A certificate or other form of recognition	19%
Practical demonstrations and real-world attack scenarios	63%
Other	2%
Q10: Do you think teachers should be required to undergo training in cybersecurity?	
Yes, definitely	58%
Rather yes, but voluntarily	40%
No. I don't see the need	1%
I can't say / I'm not sure	2%

D. Cyberbullying and Safe Student Behavior

The sixth question focused on cyberbullying among students. The distribution of responses was relatively balanced, except for a small proportion of teachers (2%) who reported encountering this issue repeatedly. One-third of respondents indicated that they had encountered cyberbullying only a few times (34%). Another 30% had not directly observed such incidents but suspected that cyberbullying was occurring among students. The remaining

979-8-3315-7426-0/25/$31.00 ©2025 IEEE
Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:42:22 UTC from IEEE Xplore. Restrictions apply.

34% of respondents reported never encountering this issue and had no suspicions of its presence. These findings confirm that cyberbullying is not an uncommon phenomenon but rather a real part of the school environment, which teachers are to some extent aware of. Given its recurring occurrence, it is essential to provide teachers with targeted training to help them identify incidents and respond appropriately.

The seventh question examined teachers' readiness to respond if a student reported being a victim of bullying. The results show that nearly half of the respondents (45%) would act in accordance with their school's internal guidelines and the official methodological documents issued by the Ministry of Education, which is a positive sign of awareness of formal procedures. However, a significant portion of teachers reported uncertainty or insufficient knowledge of the correct response, pointing to the need for further training and methodological support in handling bullying, including its cyber forms.

The eighth question assessed students' level of digital literacy from the teachers' perspective. Most respondents viewed student awareness as partial, with room for improvement (52%). Only one-fifth of teachers considered current education on this topic to be sufficient (20%). These results suggest the necessity of systematically integrating cybersecurity topics into the curriculum, beginning at the primary school level where foundational online behaviours are established.

The eleventh question identified teachers' suggestions for increasing student safety online. The results indicate that teachers see the need for a combination of measures—ranging from student education (78%) and better parental awareness of online threats (74%) to collaboration with experts (52%). Another important factor emphasized by respondents was the need for clearly defined rules regarding the use of technology in schools (59%). These insights can serve as a basis for developing comprehensive preventive strategies at the school, regional, and national levels.

TABLE III. Cyberbullying and Students' Safe Online Behavior

Q6: Have you ever encountered cases of cyberbullying among your students?	
Yes, repeatedly	2%
Yes, but only a few times	34%
No, but I suspect it is happening	30%
I have never encountered it	34%
Q7: How would you proceed if a student came to you and reported being a victim of bullying?	
I know exactly how to proceed	24%
I would try to help, but I don't know how	23%
I would report this information to the school management	45%
I would report this information to the parents	7%
I don't know how I would react	1%
Q8: Do you think students at your school are sufficiently informed about safe behaviour on the internet?	
Yes, the school addresses this topic adequately	20%
Partially, but there is room for improvement	52%
No, most students lack sufficient awareness	17%
I can't say / I'm not sure	11
Q11 *[multi-choice]*: What measures do you think would help improve students' safety on the Internet?	
More cybersecurity education in schools	78%
Better parental awareness of online threats	74%
Stricter rules for the use of technology at school	59%
Cooperation with experts and universities that focus on this issue	52%
I have no opinion	3%

E. Demographic Data

The twelfth question provided a demographic perspective on the respondents' teaching experience. The results show that most teachers have long-term practice—more than 20 years (49%) and between 10 and 20 years (27%). This indicates that interest in cybersecurity is not limited only to younger educators. Experienced teachers are aware of the changing conditions in the digital environment and the need for continuous training, which is a positive signal for implementing professional development across different generations of teachers.

The thirteenth question focused on the professional specialization of respondents. The results reveal that interest in cybersecurity is not limited to teachers of technical subjects but is also present among educators of language, social science, arts, and natural science subjects. This confirms that cybersecurity has broad applicability among teachers and integrating it into various subjects can be an effective way of bringing the topic closer to students.

The final, fourteenth question distinguished the type of school at which teachers work. The results show that most respondents are employed at secondary schools (87%), which influences the interpretation of the survey results. It is therefore necessary to consider the specifics of the secondary school environment, as well as the differences in the educational needs of primary and secondary school students. These differences may be crucial for designing educational programs and preventive measures.

TABLE IV. Demographic Data

Q12: How many years have you been working as a teacher?	
Less than 2	5%
2 – 5	10%
6 – 10	10%
10 - 20	27%
More than 20	49%
Q13 *[multi-choice]*: What subjects do you teach?	
Technical and Professional	33%
Social Sciences	17%
Natural Sciences	27%
Linguistic	36%
Artistic	7%
Other	7%

F. Hypotheses

As part of the preparation and implementation of the questionnaire, we formulated two research hypotheses, which were subsequently tested based on the collected data. The purpose of this chapter is to present the results of the analysis concerning teachers' attitudes toward training in the field of cybersecurity, as well as to compare the level of awareness among different groups of respondents—according to their length of teaching practice and type of school.

The findings provide important insights into how the perception of cybersecurity differs among teachers with

979-8-3315-7426-0/25/$31.00 ©2025 IEEE

Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:42:22 UTC from IEEE Xplore. Restrictions apply.

varying experience and professional specialization. These results can serve as a foundation for designing targeted training programs that consider the specific needs of different groups of educators.

1) Hypothesis 1

The hypothesis assumes that teachers consider training in cybersecurity an important part of their professional preparation and that the majority are interested in such training.

This hypothesis was tested based on responses to question 10, which focused on teachers' attitudes toward mandatory cybersecurity training. The results show that 58% of respondents explicitly supported mandatory training for teachers, while 40% supported training in this area but preferred it to remain voluntary.

These findings confirm that most teachers perceive cybersecurity training as both relevant and necessary, regardless of whether it is mandatory or voluntary. At the same time, the results suggest strong potential for the implementation of training programs that reflect the current needs of teaching staff in the digital environment.

2) Hypothesis 2

This hypothesis states that teachers with long teaching experience (more than 20 years) have a lower level of knowledge in the field of cybersecurity.

To test this hypothesis, we analysed the responses of teachers who indicated that they had been working in education for more than 20 years. Out of the total of 184 respondents, this group consisted of 90 teachers (49%).

Self-assessment of teachers with more than 20 years of practice in cybersecurity, based on question 1, shows that 33% consider their knowledge good, 56% report only basic knowledge, 10% have minimal information, and 1% are not involved in cybersecurity at all.

These results do not confirm the original hypothesis that long teaching experience automatically implies a lower level of cybersecurity awareness. On the contrary, they indicate that even among experienced teachers there is an interest in this topic and room for improvement. The findings also highlight the need for targeted support of this group, especially through practice-oriented training, which received strong interest in the survey (question 9).

For a more precise assessment of Hypothesis 2, we created Table 5. This table shows how teachers with different lengths of teaching experience rated their knowledge in cybersecurity.

The data presented below confirm that the level of cybersecurity awareness is not directly proportional to the length of teaching experience.

TABLE V. Comparison of Cybersecurity Awareness Among Teachers with Different Years of Teaching Experience

Practice	Good	Basic	Low	No attention	Number
< 2	22%	78%	0%	0%	9
2 - 5	33%	44%	17%	6%	18
6 - 10	50%	44%	6%	0%	18
10 - 20	31%	61%	8%	0%	49
> 20	33%	56%	10%	1%	90

G. Reflections and Recommendations

At the end of the questionnaire, respondents had the opportunity to express their opinions, experiences, and recommendations through an open-ended question. These responses provide a valuable qualitative insight into the perception of cybersecurity in the school environment, as well as into the questionnaire itself and its processing.

Teachers highlighted the need for practical training, better awareness among all stakeholders in the education system, as well as specific challenges they encounter in practice—from insufficient protection of school systems to difficulties in addressing cyberbullying. Several respondents also expressed doubts about the anonymity of the questionnaire, which is an important suggestion for improving future data collection methodology.

These reflections represent the authentic voice of teachers and can serve as inspiration for the development of effective training programs, methodological materials, and systemic measures in the field of cybersecurity.

V. Discussion

Based on the evaluation of the questionnaire and feedback from respondents, several areas were identified that provide opportunities for adjustments and improvements in the implementation of future research activities. These recommendations are derived from practical experiences, teachers' comments, and observed shortcomings in the data collection methodology.

A. Anonymity and Respondent Trust

. Some teachers expressed doubts about the true anonymity of the questionnaire. For future research, we recommend:

- communicating more clearly the purpose of collecting demographic data and how it will be processed,
- considering the voluntary nature of selected questions, especially those involving sensitive information,
- tailoring the questionnaire to the specific target group or organization, thereby reducing the need to collect detailed personal data.

B. Universality vs. Specificity of the Questionnaire

The questionnaire was designed as a universal tool for data collection across all regions of Slovakia. While this approach allowed for broad participation, it also revealed some challenges.

For future research, we recommend:

- creating thematically focused questionnaires tailored to knowledge levels and school types,
- considering the expertise of the target group when formulating questions,
- providing explanations or examples for technical questions to enhance clarity and improve response quality.

979-8-3315-7426-0/25/$31.00 ©2025 IEEE
Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:42:22 UTC from IEEE Xplore. Restrictions apply.

C. Limitations

This study has several limitations. Although participation was anonymous, some respondents expressed concerns that demographic questions could compromise their privacy, potentially affecting their openness. The universal questionnaire design enabled broad participation but limited insight into school-specific or technical aspects of cybersecurity. Moreover, as the study relied on self-reported data collected at one point in time, it could not capture changes in awareness over time. Future research should apply more diverse sampling and longitudinal methods to improve data reliability.

These recommendations and identified limitations provide a basis for methodological improvements in future research activities on cybersecurity in the school environment. Their implementation may contribute to greater participation, reliability, and relevance of the collected data.

VI. Conclusion

Based on the analysis of responses from 184 primary and secondary school teachers, several key areas can be identified that reflect the current state of awareness, motivation, and needs in the field of cybersecurity within the school environment.

A. Teachers' Knowledge

Most respondents possess only basic knowledge in the field of cybersecurity. As many as 66% of teachers stated that they have either basic or minimal knowledge, while only a small portion considers their knowledge to be sufficient. This situation highlights a significant room for improvement, which should be addressed through regular, practice-oriented training focused on current threats and real-world scenarios.

B. Motivation for Training

Respondents identified several motivating factors that would encourage them to participate in training. The most frequently mentioned included:

- increasing their personal safety when using the internet,
- striving to be a better role model for students,
- interest in practical demonstrations and real-world attack scenarios – the most cited motivation.

From these responses, it follows that purely theoretical training is not sufficiently attractive for teachers. Educational activities should therefore reflect practical needs and experiences from teaching practice, and Virtual laboratories should be used. [5]

C. Availability of Training

As many as 40% of teachers stated that they had never attended cybersecurity training, yet they expressed interest in participating if such training were available in a practical form. This finding highlights the insufficient availability of training, which should be systematically integrated into the continuing education of teaching staff

The results of Question 10 further show that 58% of respondents support mandatory training, while another 40% consider it important as part of voluntary professional development. Teachers are therefore aware of the importance of education in cybersecurity, and a large proportion of them are willing to participate in it on a regular basis.

D. Preferred Training Topics

The most preferred topics included:

- prevention of cyberbullying among students,
- phishing and other types of attacks,
- methods of protection against online threats.

These topics show that teachers seek practical information useful for both self-protection and student education

E. Cyberbullying in the School Environment

Teachers' responses clearly indicate that cyberbullying is a real issue within the school environment. More than half of the respondents have either directly encountered it or suspect its occurrence.

At the same time, several teachers admitted that they are uncertain about how to respond appropriately in such cases. This highlights the need for clear methodological guidelines that would inform teachers of their legal and professional responsibilities when addressing cyberbullying.

It is therefore essential to devote increased attention to this area, particularly to ensure timely, professional, and coordinated intervention by educators when cyberbullying is suspected or detected in schools.

Acknowledgement

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I05-03-V02-00010.

References

[1] "Cybersecurity Competence Center UNIZA." Accessed: Oct. 03, 2025. [Online]. Available: https://kc.uniza.sk/

[2] A. Ibrahim, M. McKee, L. F. Sikos, and N. F. Johnson, "A Systematic Review of K-12 Cybersecurity Education Around the World," *IEEE Access*, vol. 12, pp. 59726–59738, 2024, doi: 10.1109/ACCESS.2024.3393425.

[3] S. Scholefield and L. A. Shepherd, "Gamification Techniques for Raising Cyber Security Awareness," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Verlag, 2019, pp. 191–203. doi: 10.1007/978-3-030-22351-9_13.

[4] Y. K. Peker, L. Ray, and S. Da Silva, "Online cybersecurity awareness modules for college and high school students," in *Proceedings - 2018 National Cyber Summit Research Track, NCS 2018*, Institute of Electrical and Electronics Engineers Inc., Dec. 2018, pp. 24–33. doi: 10.1109/NCS.2018.00009.

[5] J. Jurc, M. Sterbak, and M. Kontsek. "Virtual laboratories and their usage in university environment." In 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), pp. 260-265. IEEE, 2020.

979-8-3315-7426-0/25/$31.00 ©2025 IEEE
Authorized licensed use limited to: University of Zilina. Downloaded on December 22,2025 at 10:42:22 UTC from IEEE Xplore. Restrictions apply.