FUTURE LAW
WORKING PAPERS 2024 • 4

universität
innsbruck
Institut für Theorie
und Zukunft des Rechts

MATTHIAS C. KETTEMANN • MALTE KRAMME
CLARA RAUCHEGGER • CAROLINE VOITHOFER
EDITORS

# Evaluating the need for cybersecurity teaching materials for schools

ASTRID BÖTTICHER

INNSBRUCK

MAY 2024 • ZUKUNFTSRECHT@UIBK.AC.AT

FUTURE LAW
WORKING PAPERS 2024 • 4

MATTHIAS C. KETTEMANN • MALTE KRAMME
CLARA RAUCHEGGER • CAROLINE VOITHOFER
EDITORS

universität
innsbruck
Institut für Theorie
und Zukunft des Rechts

The Future Law Working Papers was established in 2022 to offer a forum for cutting-edge research on legal topics connected to the challenges of the future. As the German Constitutional Court recently ruled, we have to act today to save the freedoms of tomorrow. Similarly, the Future Law Working Papers series hosts research that tackles difficult questions and provides challenging, and at times uncomfortable, answers, to the question of how to design good normative frameworks to ensure that rights and obligations are spread fairly within societies and between societies, in this generation and the next. The series is open for interdisciplinary papers with a normative twist and the editors encourage creative thinking. If you are interested in contributing, please send an email to the editors at zukunftsrecht@uibk.ac.at. Submissions are welcome in English and German.

The series is edited by the senior members of the Department of Legal Theory and the Future of Law at the University of Innsbruck, Matthias C. Kettemann, Malte Kramme, Clara Rauchegger and Caroline Voithofer.

Founded in 2019 as the tenth department of the law faculty, the Department of Legal Theory and Future of Law at the University of Innsbruck (ITZR) investigates how law can make individuals as well as society, states as well as Europe "fit" for the future and if and how law has to change in order to meet future challenges. This includes the preservation of freedom spaces as well as natural resources in an intergenerational perspective, the safeguarding of societal cohesion in times of technologically fueled value change, the normative framing of sustainable digitization and digitized sustainability, and the breaking through of traditional legal structures of domination and thought with a view to rediscovering the emancipatory element of law against law.

Publisher: Institut für Theorie und Zukunft des Rechts, Universität Innsbruck
Innrain 15, 6020 Innsbruck
Univ.-Prof. Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard)
Univ.-Prof. Dr. Malte Kramme
Ass. Prof.$^{in}$ MMag.$^{a}$ Dr. Clara Rauchegger, LL.M. (Cambridge)
Univ.-Ass.$^{in}$ MMag.$^{a}$ Dr.$^{in}$ Caroline Voithofer

Erasmus+ Project
EnCycLEd
Enhancing Cybersecurity Literacy in Education

Co-funded by the European Union

# Evaluating the need for cybersecurity teaching materials for schools

Astrid Bötticher

**Abstract:** This study aims to gain a comprehensive understanding of the requirements of course modules that deal with critical cyber security issues. It uses a broad definition of cybersecurity that goes beyond the technical perspective typically used in such discussions. The study examines the current state of cybersecurity education in schools, focusing on various aspects such as the quality of teaching materials, the topics taught, the distribution of topics, and the rating of topics by teachers. The study examines then the extent to which the respondents consider various topics to be important for cyber security education in schools.

Keywords: Cybersecurity; Teachers; Education; Course Topics; Course Materials

## 1. Introduction

In the contemporary world, cybersecurity is of paramount importance due to the pervasive use of technology, which has rendered social activities more reliant on online platforms. However, this increased reliance also renders individuals and organizations susceptible to cyber threats. Cyber attacks not only compromise sensitive data but can also harm relationships [1]. Conducting research surveys assists in identifying current challenges and trends in cybersecurity and provides valuable insights for developing effective cybersecurity teaching materials and enhancing cybersecurity education and practices. Many of the previous studies address the needs of children [2] [3]or look at experts [4]. This is correct and important, but another important group for education is the group of teachers. We see currently a focus in research on teachers within universities [5] or a focus on what obstacles exist to teach cybersecurity in secondary school education [6]while others have become outdated in

[1] Bendiek, A., & Bund, J. (Hosts). (2023, September 28). Learning to live with the threat? Understanding Europe's cyber defense approach [Audio podcast episode]. Retrieved from https://eurepoc.eu/de/publication_de/learning-to-live-with-the-threat-understanding-europes-cyber-defense-approach/

[2] Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, 100343.

[3] Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., Serry, E., Trotter, S., Spanos, T., & Rogic, N. (2022). Best Practice Framework for Online Safety Education: Results from a rapid review of the international literature, expert review, and stakeholder consultation. International Journal of Child-Computer Interaction, 33, 100474. https://doi.org/10.1016/j.ijcci.2022.100474

[4] Chaudhary, S. (2024). Driving Behaviour Change with Cybersecurity Awareness. Computers & Security. Advance online publication. https://doi.org/10.1016/j.cose.2024.103858

[5] (Dragoni, N., Lluch Lafuente, A., Massacci, F., & Schlichtkrull, A. (2021). Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]. IEEE Security & Privacy, 19(1), 81-88. https://doi.org/10.1109/MSEC.2020.3037446

[6] 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

a constantly changing technological environment [7]yet research shows, that cybersecurity as a topic within secondary school education is a pressing need.

The EnCycLEd Erasmus+ Project (grant number “2023-1-AT01-KA220-SCH-000166888). aims to develop and pilot teaching materials for schools. A survey was launched to get an idea of how teachers perceive the current situation of cybersecurity education and what topics teachers, parents and educational staff consider important in cybersecurity education in the future as well as what kind of teaching materials teachers prefer.

The first objective of this study is to gain a more comprehensive understanding of the potential requirements for course modules addressing critical cybersecurity topics. To this end, we have adopted a broad definition of cybersecurity that extends beyond the technical perspective typically employed in such discussions. For instance, we have not limited our scope to the narrow definition of cybersecurity as "the technologies and practices that protect data as well as computer and network systems," as proposed by Wang, Yang, and Wan [8]. The understanding of cybersecurity on which this study is based also includes human aspects like social engineering practices and cannot be reduced to secure programming or technical artifacts alone [9]. Scientists Knockaert et al. point out: "Cybersecurity is an imperative that must be placed at the service of fundamental rights and must ensure their effectiveness, in particular the right to privacy, the right to the protection of personal data, the right to freedom of expression and the right to non-discrimination"[10]. In its regulation, the European Parliament set forth an idea of cybersecurity to which our understanding can be related [11]. Our definition of cybersecurity is therefore entirely compatible with the understandings of cybersecurity as it outlined by cybercriminology [12].

[7] Xu, L., & Xue, P. (2012). The research on teaching resource development and its application effect in middle and primary schools. In 2012 International Conference on Systems and Informatics (ICSAI2012) (pp. 1030-1033). Yantai, China. https://doi.org/10.1109/ICSAI.2012.6223188

[8] Wang L, Yang J, Wan P-J. Educational modules and research surveys on critical cybersecurity topics. International Journal of Distributed Sensor Networks. 2020;16(9). doi:10.1177/1550147720954678

[9] Federal Office for Information Security. (n.d.). Social engineering - the human being as a weak point. Retrieved April 26, 2024, from https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social_engineering.html

[10] Knockaert, M., Gyseghem, J. M. van, Friedewald, M., & Lindner, R. (n.d.). Ethical, legal and societal aspects. Retrieved from https://publica.fraunhofer.de/handle/publica/300596

[11] European Parliament, & Council of the European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151/15.

[12] Rüdiger, T.-G., & Bayerl, S. (2020). Cyberkriminologie: Kriminologie für das digitale Zeitalter. Springer VS.

The second objective of this study was to identify the extent to which teachers and other stakeholders perceive a need for cybersecurity materials and thirdly to gain insight into the current state of cybersecurity education in schools. An understanding of the extent to which educators and other stakeholders perceive a need for cybersecurity materials is essential for the development of educational resources that are both effective and appropriate. It is of paramount importance to gain insight into the current state of cybersecurity education in schools in order to develop effective strategies to enhance cybersecurity in the classroom and identify teachers needs [13]. A fourth objective was to find out, which kind of materials teachers would like to utilize during class. It was crucial to identify which materials teachers would prefer to utilize in the classroom in order to align their instruction with their own and students' needs and to create learning and living environments that are as student-oriented as possible [14].

The findings of this survey could inform the development of targeted measures to enhance cyber security education in schools. They could identify areas of vulnerability and highlight the necessity for additional resources. They could also discover how teachers perceive the existing materials and detect potential areas for improvement as well as delivering materials that are reflecting the current cybersecurity situation and accommodate students' information habits.

## 2. Materials and Methods

We conducted a Survey via Lime-Survey from 29.01.2024 – 15.02.2024. The statistics presented in this document have been developed using a frequency distribution, which represents the answers to the research question.

The survey was divided into three sections. The first part was dedicated to the respondents themselves in order to capture a picture of the group. We asked about age and gender and whether our respondents were actually teachers or had any other connection to children. Those who stated that they were teachers were asked

[13] Rahman, N. A. A., Sairi, I. H., 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. ISSN: 2010-3689. https://doi.org/10.18178/ijiet.2020.10.5.1393.

[14] Childers, G., Linsky, C. L., Payne, B., Byers, J., & Baker, D. (2023). K-12 educators' self-confidence in designing and implementing cybersecurity lessons. Computers and Education Open, 4, 100119. https://doi.org/10.1016/j.caeo.2022.100119

questions about their school (e.g. differentiation by city/state) and the type of school. Those who stated that they were not teachers were asked about their contact with children (e.g. educators, family ties). The teachers were asked which cyber security topics are taught today and how they would rate the teaching material. One question we asked teachers and non-teachers alike was which cybersecurity topics were important for teaching and asked our respondents to rank each topic (1 - not important/ 10 - very important). In addition, everyone was asked equally which teaching materials they considered appropriate for pupils today, i.e. which methodological material should be used.

## 3. Results

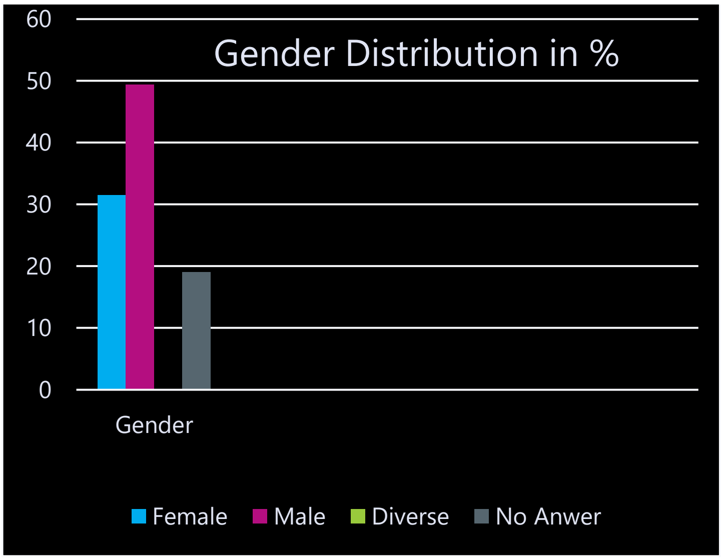
### 3.1. Respondents

It was crucial to understand who our respondents generally are, what age and gender attributes they have and if they are teachers, from what kind of school they come from.

#### 3.1.1. Gender Distribution

The survey was completed by a total of 251 people, with 174 complete questionnaires and 77 incomplete questionnaires returned. The people assigned themselves to the female gender (79) and the male gender (124) or did not provide any information (48), while no one assigned themselves as diverse. This means that we have an overrepresentation of men.

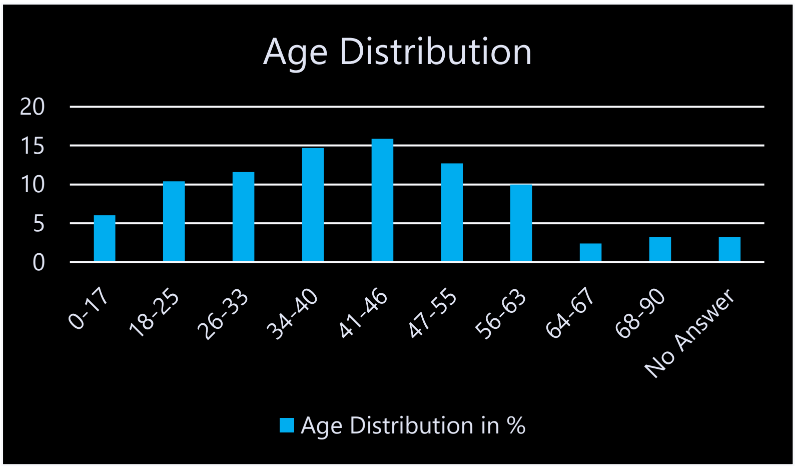
Gender Distribution among Respondents



### 3.1.2. Age Distribution

The 41-46 age group was the most strongly represented (40 people), followed by the 34-40 age group (37), the 47-55 age group (32), the 26-33 age group (29), the 18-25 age group (28) and the 56-63 age group (25). This age structure probably reflects the professional commitment of the interviewees, as the entry into and exit from the profession in the age groups surveyed here again coincide. It is noteworthy that 15 individuals indicated the age group 0-17, while the individuals in the age groups after retirement (63-67 and 68-90) altogether comprised only 14 people. This could suggest a general interest in cybersecurity among young people. Only 8 individuals did not provide their age.

Age Distribution among Respondents



For consideration, it is also important to note that the majority of respondents do not work as teachers (67 teachers compared to 142 individuals) but are particularly involved with children or adolescents for family reasons (81 individuals) or work in another educational profession (39). This suggests that especially individuals personally affected took part in the survey. The time when individuals start their own families and have interactions with children and adolescents might be reflected in the age structure of the interviewees.

### 3.1.3. Representation of School types

Regarding the teaching staff, the type of Vocational School is overrepresented with 49 respondents, while all other types of schools were underrepresented with 16 respondents in total. This means that the questions specifically directed towards teachers primarily reflect experiences from the Vocational School educational setting, and we cannot draw a comprehensive picture for all other types of schools. The statements can only be related to this specific type of school. Differences based on rural and urban settings cannot be depicted either, as we have an overrepresentation of urban schools: 61 teachers stated that their school is located in a city, while only 2 were in a suburb or rural area (3).

## 3.2. Teaching Cybersecurity Today

In order to understand the current situation today regarding cybersecurity teaching in schools, we have developed a section of the survey, where correspondents were able to give feedback on their general view, on topics that are already being teached in the classroom. This was important as we needed to gain a general overview of the current situation that students and teachers experience.

### 3.2.1. Rating the Teaching Material

As part of the present study, the quality of cyber security teaching was assessed by the respondents. This question was only asked to those who had indicated that they were teachers and only those, that answered, that cybersecurity is taught currently or in the past. The 67 surveyed teachers evaluated the current educational materials for the field of cybersecurity in general. It was important for us to assess how the teaching was generally perceived in order to obtain a general quality assessment.

We asked for the “Current situation regarding cybersecurity education in school”.

In 62.7% of the responses of the teachers, interviewees indicated that cybersecurity is taught in the curriculum, while 23% stated that there is no cybersecurity education at all, and 11.9% of the respondents were unsure. Those that stated, that cybersecurity is part of the education in their school, we asked further: How is the current state of the available teaching materials for cybersecurity topics used in school?

**Table 1**. General Evaluation of teaching material

How is the current state of the available teaching materials for cybersecurity topics used in school?

| | |
|---|---|
| Poor | 3 % |
| Fair | 9 % |
| Average | 35,8 % |
| Good | 11,9 % |
| Excellent | 0 % |

A general level of satisfaction was found among those who stated that cyber security was part of the curriculum and assessed the materials used. The assessment clearly shows that a considerable amount is already being done in European education and that schools are active and that teaching material is generally average to good. However, it is important to note here that a large number of schools do not offer any lessons on the subject at all - almost a quarter of those surveyed stated this. This shows how important it is to bring cyber security as a topic into schools and to provide teachers with offers that make their everyday life and the conception and preparation of lessons easier. Among the respondents who indicated that there is teaching, none stated that there is excellent material, and only 11,9% acknowledged the material to be of good quality. This indicates that good material not only needs to be urgently developed but also requires targeted measures for its distribution.

### 3.2.2. Topics Taught

It is crucial to ascertain which topics have already been taught in order to identify potential areas of deficiency or unmet need for additional resources. This allows for targeted efforts to enhance cybersecurity education and ensure that students gain a comprehensive understanding of the subject matter.

We asked about the “Current situation regarding cybersecurity education in school” and explained why we asked this question with the following text: “Cybersecurity plays a crucial role in today's digital landscape. Your input on whether schools provide cybersecurity education is valuable for understanding the current state of digital literacy.“

In our survey, a simple list of possible topics was compiled and presented to the respondents, who were then able to make multiple selections. The question "Which of the following cybersecurity topics are taught?" aimed to understand the current status quo and determine which topics in the field of cybersecurity are already covered in the curriculum. Based on this, targeted measures can be taken to address any gaps and improve cybersecurity education for teachers. We named 14 Items that could be of importance to students.

### 3.2.3. Queried Topics

The topic rules and regulations on the internet is important as it gives pupils an understanding of the legal framework of the internet, which is essential for safe and responsible behavior in the digital space. It was therefore important to see whether schools already offer this topic. Data protection is a fundamental concept that is important to protect personal information and be aware of how information can be used online (also against a person). The topic Internet safety (information about harmful behavior on the Internet) is important to protect oneself from potentially dangerous online situations. The techniques and tactics used by attackers to manipulate students, or put them under pressure or steal sensitive information is important and therefore it was crucial to understand if awareness of social engineering is taught at school. Managing passwords correctly is crucial to keeping online accounts secure and know how to prevent unauthorized access, so this topic was queried to find out if students today are learning how to create secure passwords. To teach students how to communicate safely online without revealing personal information or falling victim to fraud is in line with the habits of young people to exchange information online and to live their lives in digital spaces such as social media platforms. With the increasing use of AI technologies, it is important that students are aware of the potential dangers associated with the manipulation of images and sound by AI and learn that not everything on the web is 'real information'. Asking about this topic was important to find out whether students are informed about the impact of AI-based attacks and understand how they can protect themselves against them. The topic incident response and management is teaching students to learn how to respond appropriately to security incidents and manage them effectively in order to minimize damage. The security of mobile devices such as smartphones and tablets is crucial in today's connected world and is becoming increasingly important, especially for young people, as it is very much in line with young people's lifestyles. Digital citizenship and responsible online behavior is important for students to understand their role as responsible and ethical participants in the digital space, while malware and viruses are common threats to cyber security that can have serious consequences. Ethical hacking addresses the methods and techniques used by ethical hackers to identify and fix security vulnerabilities. Algorithmic decision making and behavior addresses the ethical and social implications of algorithmic decisions and their impact on human behavior. In the context of cybersecurity education, this topic is of interest in order to understand if students are being teached today on the influence of algorithms on decision-making processes. Blockchain technology has applications in various fields and requires an understanding of the security aspects for secure application. The question was posed as to whether cybersecurity education currently being taught is existent to ensure that students are developing an understanding of the security aspects of blockchain technology and learning about it at school. Financial transactions and online-shopping is a daily activity for the majority of society, this is why financial cybersecurity and prevention of online financial crimes could be relevant within teaching concepts today. To develop digital competency and protect financial and personal data is a crucial knowledge to develop resilience.

## 3.3. Topic Distribution in Cybersecurity Education

In order to understand the current situation today regarding cybersecurity teaching in schools, we have developed a section of the survey, where correspondents were able to give insights on the current topics that are part of cybersecurity education today.

### 3.3.1. Which topics are taught?

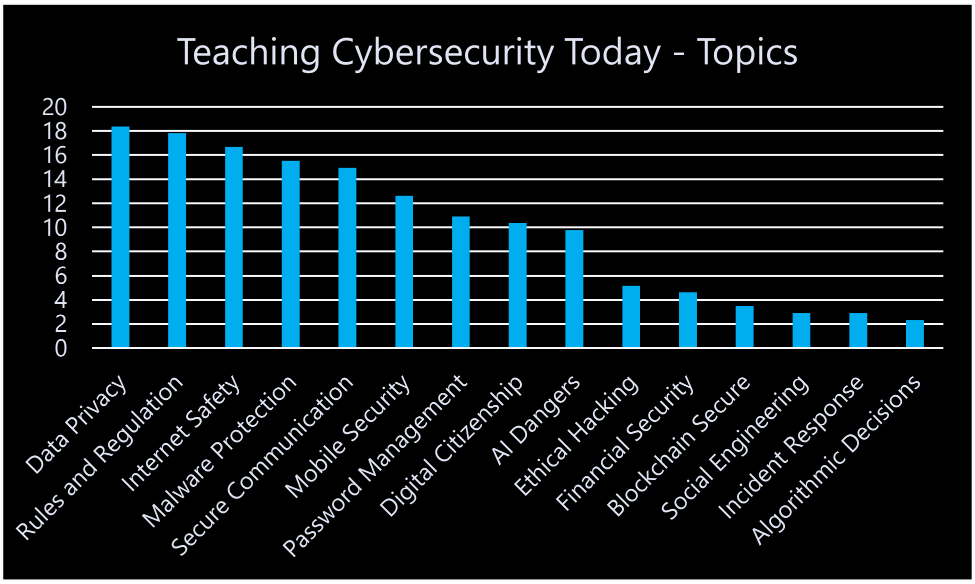
We observe a relatively balanced range of topics in the distribution of taught content. It is noticeable that particularly the topics requiring relatively high technical expertise are taught less frequently than those that involve more social aspects. We asked those who indicated that cybersecurity is taught at school which topics are being taught. Only close-ended answers were possible and multi-selection was possible.

**Table 2.** Which of the following cybersecurity topics are taught?

| Topic | Quantity of Votes | Gross Percentage |
|---|---|---|
| Rules and regulations of the Internet | 31 | 17.82 % |
| Data Privacy | 32 | 18.39 % |
| Internet Safety (Information about predatory behavior online) | 29 | 16.67 % |
| Social Engineering Awareness | 5 | 2.87 % |
| Password Management | 19 | 10.92 % |
| Secure Online Communication | 26 | 14.94 % |
| Dangers of artificial intelligence (e.g. image and sound manipulation) | 17 | 9.77 % |
| Incident Response and Management | 5 | 2.87 % |
| Mobile Security | 22 | 12.64 % |
| Digital Citizenship and responsible online behavior | 18 | 10.34 % |
| Protection against malware and viruses | 27 | 15.52 % |
| Ethical Hacking and Penetration testing | 9 | 5.17 % |
| Algorithmic Decision-Making and behavior | 4 | 2.30 % |
| Blockchain Security | 6 | 3.45 % |
| Financial Cybersecurity and Prevention of Online Financial Crimes | 8 | 4.60 % |

Data privacy, internet rules, and secure online communication seem to be taught particularly frequently. This could indicate that these topics are considered especially relevant or fundamental. Some specialized subjects like Blockchain Security or Algorithmic Decision-Making are taught less frequently. This might suggest that there is potentially less focus or resources dedicated to these specific areas. However, the broad range of topics covered indicates that schools are making efforts to provide students with a comprehensive understanding of cybersecurity. Some schools may emphasize technical aspects more, while others focus more on behavioral aspects. The high number of non-responses in this case is because only teachers were asked this question. If someone did not explicitly indicate being a teacher, this question was not presented to them. Thus, we have a picture of those who are professionally active in the school environment. Yet, the results may indicate that certain topics in cybersecurity need to be emphasized more to strengthen the awareness and knowledge of teachers.

Topic Distribution within Cybersecurity Education Today



The visualization allows more easily to identify the distribution of various topics. It is evident that there is a notable disparity in the representation of cybersecurity topics in schools. While social engineering topics such as cybergrooming, data theft, and fraud are crucial, as our respondents indicated, social engineering practices are not consistently taught or are not taught frequently. There is a notable discrepancy between the desired content and the content of previous lessons. At this juncture in the survey, the term "social engineering" has not been reiterated in parentheses. However, since the term was introduced as part of the survey, it can be assumed that teachers deliberately pointed out the absence of these topics.

### 3.4. Topic Rating in Cybersecurity Education

We wanted to understand what topics teachers regard as valuable and useful for cybersecurity education. In order to test to what extent the distribution changes, and how specific the answers of our respondents are, we tested the response data using various means. In addition to the highest approval rate, we also analyzed the data again according to high approval rate and disagreement.

#### 3.4.1. Highest Approval Rates

Respondents were asked to select from a list of 13 possible topics for teaching cybersecurity in schools those they considered important and to rate them on a scale of 1 (not at all important) to 10 (particularly important). The answers were given using the Lickert scale. The Lickert Scale employs a standardized measurement method that enables respondents to differentiate between the various topics with greater precision. Its straightforward nature facilitates respondents' comprehension and use, thereby reducing the likelihood of misinterpretation.

We asked all our respondents which topics they felt were important for teaching cyber security in schools and asked them to rate them from 1 (not at all important) to 10 (particularly important). We asked for 13 possible topics for which an assessment could be made. The topics included the following items: Cybergrooming, Social Media, Online Behavior, Risk Management, Rules and Regulations (criminal liability), Ethical hacking, Phishing, Malware and Virus Protection, Mobile Security, Cloud Security, IoT, AI-generated content (social bots/fake videos, images, voices), Basic Understanding of Artificial Intelligence, algorithmic decisions and their significance for behavior. To prevent any potential confusion, illustrative examples have been included in parentheses for certain items in order to provide a clear and unambiguous interpretation.

The following is the question that was posed: Which cyber security topics do you think are particularly relevant to the secondary school curriculum? 1= not important at all -

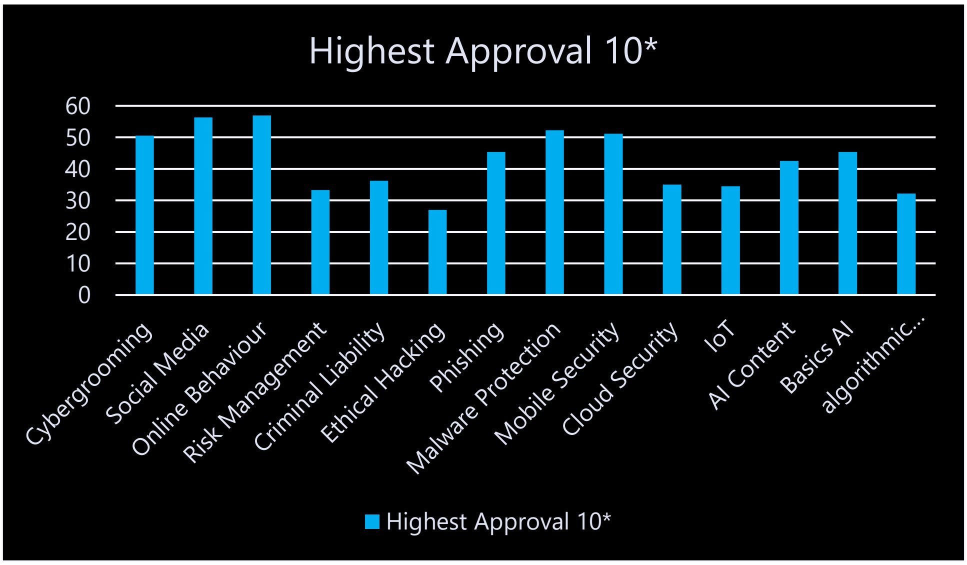
10= most important. Based on the highest approval rating (10*) of the respondents, we have ranked the different topics displayed in the survey.

**Table 3.** Relevancy of Topics of Cybersecurity Education

| Topic | Agreement Rate in Percentage |
|---|---|
| Online Behavior | 56.90 % |
| Social Media | 56.32 % |
| Malware and Virus Protection | 52.30 % |
| Mobile Security | 51.15 % |
| Predatory Behavior (Cybergrooming) | 50.57 % |
| Phishing | 45.40 % |
| Basic Understanding of Artificial Intelligence | 45.40 % |
| AI-generated content (social bots/ fake videos/ images/ voices) | 42.53 % |
| Rules and Regulations (criminal liability) | 36.21 % |
| Cloud Security: | 35.06 % |
| Internet of Things | 34.48 % |
| Risk Management | 33.33 % |
| Algorithmic decisions and their significance for behavior | 32.18 % |

The ranking could indicate that teachers place particular emphasis on topics related to human behavior and social media, as this is perceived as the greatest uncertainty or danger and is heavily discussed in politics as well as in the media – related to fake news, polarization and issues connected. The fact that topics such as "Social Media", "Online Behavior" and "Malware and Virus Protection" are in the top positions could indicate that the focus is on how human behavior and social interactions in the digital space can pose potential dangers to individuals as well as society. Human-machine-human interaction plays a role in the first two topics, while malware and virus protection points to human-machine communication and is named the third topic with highest approval rate. Malware and viruses are prevalent cybersecurity threats that can have severe consequences. The level of damage caused by malware and viruses can be extremely high. It can have severe consequences, ranging from data breaches and unauthorized access to financial losses and disruption of critical systems. In the modern digital landscape, mobile devices are widely used, and securing them is crucial to the society in general. The inclusion of "Mobile Security" in the top rankings may reflect the acknowledgment of the significance of securing devices like smartphones and tablets especially for students. This reflects that our respondents have based their ranking on a real world relevance and the ranking displays this real world relevance. The last mentioned item, ethical hacking, still has the highest relevance for nearly a third of the respondents.

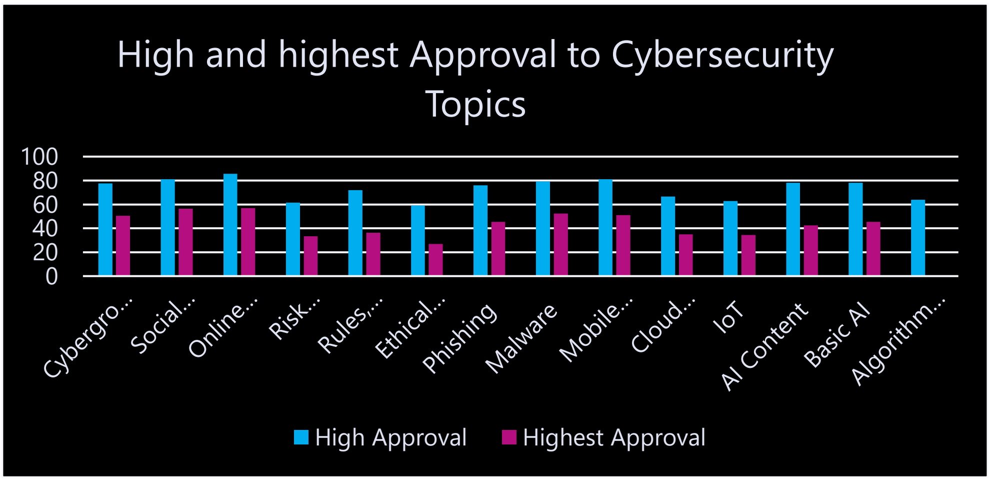
Topic Distribution within Cybersecurity Education Today



### 3.4.2. High Approval Rates

To provide a comprehensive overview of the level of agreement among respondents regarding the importance of various cybersecurity topics highest and high approval rates are measured and presented together. This chart shows the different approval ratings: Blue shows the high agreement (8*,9*10*) and red the highest agreement (10*) with the topics that could be taught in cyber security lessons. If the respondents' approval ratings were high, we rated the approval rating 8* or higher. It is striking that all topics were considered important by the respondents and that the lowest approval rate of a topic with 59.19% approval value (ethical hacking) can still be considered relatively high important, so that although the respondents presented a clear opinion, each of the topics mentioned in the questionnaire was considered highly important and of the utmost importance by the majority. This suggests a clear consensus among the respondents regarding the significance of cybersecurity as a topic. Interesting is that the highest and the high approval rates essentially mirror each other. This suggests a strong consensus on which topics are considered particularly relevant for cybersecurity education.

Distribution of Approval of Topics



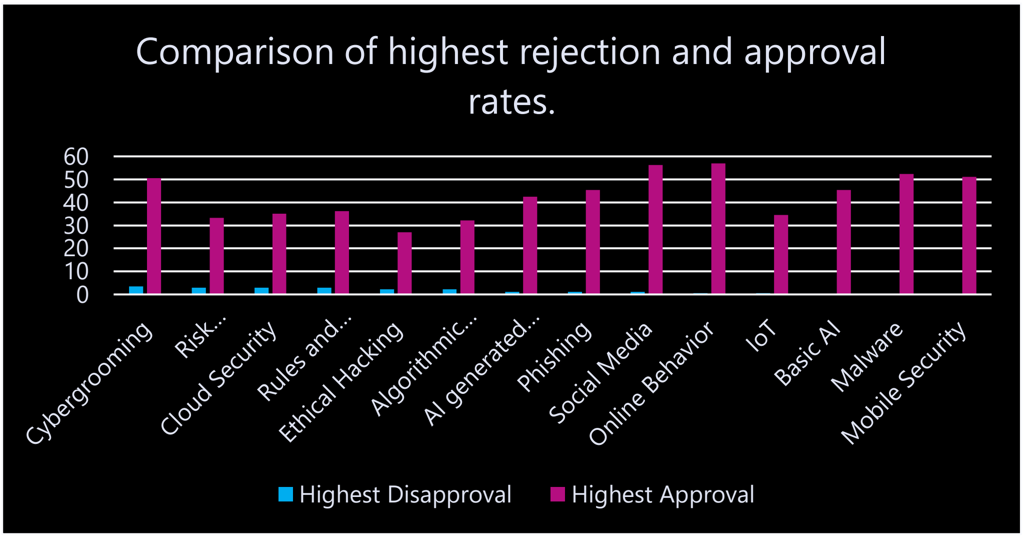
The results could indicate that the amount of material to be taught is perceived as extensive and that there may be difficulties in prioritizing: It is possible that the high approval rates are related to the excessive demands placed on teaching staff to prioritize given the volume of material to be taught. A positive perspective could be that the high ratings reflect the growing importance of cyber security and computer science in education. This could indicate that teachers recognize the need to fully prepare students for the challenges of the digital world. The result can also be interpreted as a clear indication that the preparation of pupils in digital topics is taking on an increasingly important perspective and that abbreviated lessons - which necessarily have to live with gaps - are not considered desirable. The generally high approval rates also suggest that the respondents may not have a clear overview of the truly central topics in cybersecurity and youth protection – everything is considered 'somehow important.' Yet, this could also be a sign, that cybersecurity is highly relevant for schools and youth in general and that there is a great need to enhance teaching (time/topics a.s.o.). Generally, the data could point to the fact, that the difference between online and offline world is diminishing and that schools are in a great need to prepare its students for a future, where life is partly lived in the online world.

### 3.4.3. Rejection Rates

In this context, the (albeit very low) rejection rates are also important, as they provide a very interesting picture and help to interpret the data. For example, the topic of cybergrooming was rated as highly important (8* or above) by 77.58% of respondents, putting it in 6th place among the most important topics, while at the same time it received the highest rejection rate of 3.45%. Cybergrooming had with 50,57 % highest approval a relatively high 5th position in the ranking of topics according to highest approval rates. The low approval rates can be interpreted in various ways. Some respondents might be unsure about which topics are particularly important and, therefore, may tend to give lower rejection rates to avoid taking a clear position. Respondents may have varying levels of expertise in different subject areas. Therefore, they might hesitate to rate certain topics as 'not important' if they don't feel confident in that specific area. Some respondents may be unsure about certain topics, leading them to hesitate in categorizing them as 'not important.' This is particularly true for complex or specialized areas of cybersecurity that are less commonly taught or discussed. It is evident that cybersecurity topics are often perceived as "expert topics" and require enhanced communication to the general public. Teachers, as communicators, and their pivotal role as multipliers, play a crucial role in this regard. The promotion of teacher knowledge is an essential factor in promoting a cybersecurity-conscious society. Childers, Linsky, Payne, Byers, and Baker (2023) examined K-12 educators' confidence in designing and implementing cybersecurity lessons (Computers and Education Open, 4, 100119).

The high approval rates for topics and the very low rejection rates can be interpreted together. The avoidance of negative rates may also be linked to a broader educational agenda that seeks to impart a more diverse range of knowledge in academic settings. It is possible that they may prima facie prefer to abstain from categorizing topics as "not important," particularly if they perceive them as potentially significant to cybersecurity education. It is yet also possible that respondents may desire comprehensive cybersecurity education that encompasses a wide range of topics, despite feeling less confident about certain areas. Consequently, they may be inclined to avoid rejecting topics outright in order to ensure that all relevant aspects are considered and addressed.

Comparison of Distribution of Approval and Rejection



As soon as we divided the material into approval or rejection - i.e. a rating of 1-5 rejection and 6-10 approval as approval - the indecision about the "right" choice of topic becomes even clearer, because we receive high approval ratings for all the topics available for selection. This reinforces the picture that our respondents were not only undecided, but that there may be a lack of orientation. In the hot-or not topic, all topics were important to our respondents. This indicates that teachers are also important target groups for bringing cyber security into schools. They need more specialized information and didactic and methodological tools to make it easier for them to deal with this difficult topic. This includes exchanging ideas with other teachers, making it easier to find relevant information and understanding why cyber security is important and how it can be taught. However, this also demonstrates the importance of cyber security in the lives of teachers and students today. They urgently need answers and guidance in all areas of cyber security, because cyber security is becoming increasingly important due to the installation of intelligent systems in all areas of modern society. This dependence on all intelligent systems in the lives of students and teachers is therefore also strongly indicated here.

### 3.5. Teaching Material Preferences

Identifying preferences about teaching materials was crucial to ensure that cybersecurity lessons were tailored to the needs and preferences of teachers and students and provided an optimal learning experience. It is crucial to identify the needs of teachers in order to convey cybersecurity in such a way that the materials can be effectively used in the classroom. Achieving outstanding learning outcomes is only possible when the teaching material is tailored to the life situation and learning habits of learners and teachers.

#### 3.5.1. Teaching Material Preferences

We asked all respondents about the materials they would consider valuable for effective cybersecurity education. We utilized the option for multiple responses and provided methodological materials for teaching. Multiple selections were allowed and we received 1200 responses in total. In relation to the methodological materials that should be used in teaching, there was a very clear picture. Among the fourteen items, six received lower rates than 50% of respondents selecting them as valuable resources for cyber security education. This pattern indicates a preference for interactive and engaging learning materials that resonate with the daily experiences of students. The emphasis on real-life scenarios in teaching materials may be a reflection of teachers' desire to provide students with practical experience. The preference for real scenarios and hands-on learning methods may indicate that teachers emphasize the importance of concrete, application-oriented content to better prepare students for real life cybersecurity challenges. It is important to note that here, our respondents were decisive, and we received a very clear picture about teaching material connected to teaching methods that are seemingly preferred.

**Table 4.** Teaching Material Preferences.

| Teaching Material | Approval Rate |
|---|---|
| Instructional videos | 74.71 % |
| Real-world cybersecurity scenarios | 66.09 % |
| Gamified learning experiences | 63.79 % |
| Interactive simulations | 61.49 % |
| Presentations | 61.49 % |
| Simulation of cyber attacks | 60.92 % |

| | |
|---|---|
| Interactive online platforms | 60.92 % |
| Online quizzes or assessments | 50.00 % |
| Group projects | 45.98 % |
| Webinars or virtual events | 40.80 % |
| Case studies | 35.63 % |
| Multiple choice sheets | 24.14 % |
| Worksheets | 23.56 % |
| Reading materials or articles | 20.11 % |

## 4. Conclusion

Approximately one-third of all respondents stated that cybersecurity is already a subject or a course in school. This means that a majority of our respondents indicated that cybersecurity is not a topic in schools or is not taught. This is an important indication that schools need to be better prepared on the topic of cybersecurity, and there must be urgent provision of materials and opportunities to facilitate schools in preparing their students for digital life and the existing dangers. For teachers, it is important that cybersecurity is not treated solely as a technical topic but that cyber threats carry a social component that should be part of the curriculum in schools. An important source of information about online dangers is cyber criminology, which can delineate the criminal phenomena that have developed in the digital realm. However, teachers also emphasize that basic knowledge should become a central part of the curriculum and resilience should be built within the student body: this includes securing passwords as well as considering which data is shared with whom and what consequences could arise from it. Anticipating future dangers resulting from one's own behavior (e.g., sharing images or audio recordings online) is just as important as building resilience regarding the devices regularly used by students. Additionally, helping students behave "correctly" and showing them the possibilities and limits of personal actions are major topics. Therefore, teachers also wish to address the question of how to prevent deviant or even criminal behavior. This is also part of a curriculum that focuses on resilience and helps students behave in a legally compliant manner in the digital space. Introducing this topic into cybersecurity education remains a challenge, especially for Europe and schools located in Europe, as there is no European criminal law in this form and there are no generally applicable European standards that would allow for the development of universally applicable materials; rather, individual national standards must be incorporated into cybersecurity education and material development. Thus, it is necessary for nations to establish some form of repository that enables teachers to make their students aware of the boundaries of their actions in the digital space and to help them move lawfully in the digital realm.

An important insight from our survey also concerns the teachers themselves. They need to be better informed and require assistance in building expertise and exchanging ideas with other teachers. They need help in assessing security situations and specific threats to their students. Since teachers are central multipliers on the way to a secure digital society, it is particularly important to promote and further develop their competencies. They need overview knowledge and insights into current materials and actual assessments of the dangers that can be derived from certain facts or examples. This means that regular updates about the insights gathered from the digital realm should be developed especially for this group of multipliers. Material provided to teachers and schools must also meet teachers as recipients of new knowledge where they stand.

Another important insight we have drawn is from the fact that teachers specifically desire certain forms of teaching materials. They need materials that help them build concrete lessons in a didactic and methodical way, so that students are engaged from their everyday lives and their learning and viewing habits are addressed. Furthermore, our survey suggests that teachers need materials that relieve them in lesson preparation and help them bring actual problems and challenges arising from the topic of cybersecurity into the classroom despite the technically demanding and emotionally charged nature of the subject.

**Funding:** This research was funded by EnCycLEd Erasmus+ Project, grant number “2023-1-AT01-KA220-SCH-000166888”.

**Data Availability Statement:** The raw data supporting the conclusions of this article will be made available by the authors on request.

**Conflicts of Interest:** The author declares no conflicts of interest. The funder had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

## References

1. Bendiek, A., & Bund, J. (Hosts). (2023, September 28). Learning to live with the threat? Understanding Europe's cyber defense approach [Audio podcast episode]. Retrieved from https://eurepoc.eu/de/publication_de/learning-to-live-with-the-threat-understanding-europes-cyber-defense-approach/
2. Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, 100343.
3. Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., Serry, E., Trotter, S., Spanos, T., & Rogic, N. (2022). Best Practice Framework for Online Safety Education: Results from a rapid review of the international literature, expert review, and stakeholder consultation. International Journal of Child-Computer Interaction, 33, 100474. https://doi.org/10.1016/j.ijcci.2022.100474
4. Chaudhary, S. (2024). Driving Behaviour Change with Cybersecurity Awareness. Computers & Security. Advance online publication. https://doi.org/10.1016/j.cose.2024.103858
5. (Dragoni, N., Lluch Lafuente, A., Massacci, F., & Schlichtkrull, A. (2021). Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]. IEEE Security & Privacy, 19(1), 81-88. https://doi.org/10.1109/MSEC.2020.3037446
6. 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
7. Xu, L., & Xue, P. (2012). The research on teaching resource development and its application effect in middle and primary schools. In 2012 International Conference on Systems and Informatics (ICSAI2012) (pp. 1030-1033). Yantai, China. https://doi.org/10.1109/ICSAI.2012.6223188
8. Wang L, Yang J, Wan P-J. Educational modules and research surveys on critical cybersecurity topics. International Journal of Distributed Sensor Networks. 2020;16(9). doi:10.1177/1550147720954678
9. Federal Office for Information Security. (n.d.). Social engineering - the human being as a weak point. Retrieved April 26, 2024, from https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social_engineering.html
10. Knockaert, M., Gyseghem, J. M. van, Friedewald, M., & Lindner, R. (n.d.). Ethical, legal and societal aspects. Retrieved from https://publica.fraunhofer.de/handle/publica/300596
11. European Parliament, & Council of the European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151/15.
12. Rüdiger, T.-G., & Bayerl, S. (2020). Cyberkriminologie: Kriminologie für das digitale Zeitalter. Springer VS.
13. Rahman, N. A. A., Sairi, I. H., 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. ISSN: 2010-3689. https://doi.org/10.18178/ijiet.2020.10.5.1393.

14. Childers, G., Linsky, C. L., Payne, B., Byers, J., & Baker, D. (2023). K-12 educators' self-confidence in designing and implementing cybersecurity lessons. Computers and Education Open, 4, 100119. https://doi.org/10.1016/j.caeo.2022.100119