



CYBERSEC  
EDUCHECK

# REPORT

## SUMMARIZING THE OPERATION OF THE CYBERSEC EDUCHECK PROJECT IN PHASE

# 2024

### Prepared By:

Jadwiga Maj  
Karolina Kornecka-Kupiec  
Karolina Pokorska  
Mateusz Pękala  
Pavla Vybihalova  
Weronika Kędzierska  
Iwona Szczurek

PROJECT NO. 2023-2-PL01-KA210-VET-000176822



Co-funded by  
the European Union

LEADER:

Research Institute  
Europe

Coventry  
University

PARTNERS:

K R  
E A  
STOWARZYSZENIE  
KREATYWNI DLA  
BIZNESU

EUROPEAN CENTRE  
FOR CAREER EDUCATION

# REPORT SUMMARIZING THE OPERATION OF THE CYBERSEC EDUCHECK PROJECT IN PHASE

**Date:** 25/07/2024

**Leader** – Coventry University Research Institute Europe

**Partners:**

- Stowarzyszenie Kreatywni dla Biznesu (eng. Creative for Business, KREA) – Poland
- European Centre for Career Education (ECCEDU) – Czech Republic

## **I. Description of needs**

- Characteristics of study participants and their needs.

## **II. Summary of the course of activities**

- Details of recruitment (names of schools)
- Activities organized (webinars) – dates, content, participants
- Numbers on the responses obtained in the survey
- Challenges
- Suggestions

## **III. Recommendations for action 2**

- Discussions on existing challenges and opportunities related to the proposed activities.
- Defining the directions of action and identifying priority areas.
- Preparation of a list of topics for further work and establishment of a schedule of activities.
- TOPICS, what will be included in the textbook/script
- Personas profiles

## **IV. Conclusions and way forward**

- The first conclusions of the survey, giving the possibility of work for the future.

.....  
Leader's signature

# I. Description of needs



Characteristics of study participants and their needs vary significantly between high school students and high school teachers in the realm of cybersecurity education. High school students generally demonstrate a basic awareness of cybersecurity threats such as cyberbullying, privacy issues, phishing, and identity theft. They are familiar with concepts like online privacy and the risks of sharing personal information, but often lack in-depth understanding and practical application. For example, while students understand the importance of strong passwords and secure browsing, they frequently fail to consistently implement these practices in their online activities.

Knowledge gaps among students are notable, particularly in practical cybersecurity measures. Many students struggle with creating strong, unique passwords, understanding the significance of two-factor authentication, and verifying the credibility of online information sources. This lack of critical evaluation skills makes them vulnerable to misinformation and phishing attacks. Moreover, students often underestimate the long-term consequences of their online actions, such as data theft and unauthorized sharing of personal information.

Beliefs and concerns among high school students regarding technology use and cybersecurity are diverse. While they express fears about identity theft, privacy breaches, and cyberbullying, many students believe they can manage these risks independently, leading to inconsistent application of cybersecurity practices. This belief sometimes fosters a false sense of security until they encounter a direct cyber incident. Privacy invasion concerns and exposure to harmful online content shape cautious behaviors in their online interactions.

In contrast, high school teachers face challenges in effectively delivering cybersecurity education due to various factors. These include limited time dedicated to cybersecurity topics within the curriculum, outdated teaching materials, and uncertainty about their own cybersecurity knowledge. Many educators express a strong need for additional training and resources to enhance their teaching effectiveness and keep pace with evolving cyber threats. For further details, refer to Part II.



## II. Summary of the course of activities

### 01. Planning the Research on Cybersecurity Education in High Schools



The primary objective of this stage was to conduct comprehensive User Experience (UX) Research to understand the needs and challenges of teachers regarding effective cybersecurity education tools and training in secondary schools in Poland and the Czech Republic. This research facilitated the creation of detailed Persona profiles to align project outcomes with the specific requirements of end-users.

#### Research Objective

The objective of this study was to evaluate the effectiveness of current educational methods and assess the role of secondary school staff in shaping students' competences in the safe use of technology. This research provides insights to enhance cybersecurity education initiatives in high schools across Poland and the Czech Republic.



# Research Questions



**1.**

**Current Awareness:** To what extent are high school students aware of cybersecurity threats?

This question seeks to gauge the level of knowledge among students regarding potential cybersecurity risks they may encounter in their daily use of technology.

**2.**

**Knowledge Gaps:** What do high school students not know about cybersecurity?

This question explores specific gaps in students' understanding of cybersecurity principles, identifying areas where additional education and awareness efforts are needed to enhance their competence in safe technology practices.

**3.**

**Beliefs and Concerns:** What threats, fears, and beliefs do school students have that may influence their attitudes and behaviors about safe technology practices?

This inquiry aims to uncover students' perceptions and attitudes towards cybersecurity threats. By identifying their concerns and beliefs, we can address misconceptions and tailor educational strategies that resonate with their perspectives.

**4.**

**Effectiveness of Educational Methods:** To what extent do current teaching methods contribute to students' practical understanding and application of cybersecurity principles?

This question evaluates the impact of existing educational approaches on students' ability to comprehend and apply cybersecurity concepts in real-world scenarios. It assesses whether current methods effectively bridge the gap between theoretical knowledge and practical skills.

**5.**

**The Role of School Staff:** How do secondary school staff, including teachers and principals, view their current role, the challenges they face, and the potential areas for improvement in cybersecurity education in shaping students' competences in the safe use of technology?

This question explores the perspectives of school staff regarding their responsibilities and challenges in delivering cybersecurity education. Understanding their viewpoints helps in identifying support needs and areas where professional development or curriculum adjustments may be beneficial.

# Achievements of UX Research:

01

## Understanding User Needs:

Through structured interviews, surveys, and observations, our UX research provided valuable insights into the specific requirements of teachers involved in cybersecurity education. This understanding guided the design of tools that effectively meet their instructional needs.

02

## Persona Development:

Based on empirical data, we have created detailed Personas profiles that accurately represent the diverse needs and preferences of teachers. These personas serve as archetypes, guiding the design and development process towards solutions that resonate with end-users.

03

## Customization of Solutions:

Our personas derived from UX research enable the customization of cybersecurity education tools to align with the unique educational contexts of Poland and the Czech Republic. This ensures that the tools are not only functional but also user-friendly and relevant to the local educational landscape.

04

## Enhanced User Engagement:

By addressing identified pain points and aligning solutions with the personas' needs, we anticipate increased user engagement and adoption rates. Teachers are more likely to embrace and effectively utilize tools that are designed with their specific challenges in mind.

05

## Optimized Project Outcomes:

Integrating insights from UX research and persona development has optimized the effectiveness and success of the cybersecurity education initiative in secondary schools. This alignment ensures that project outcomes meet the practical needs of teachers and contribute positively to educational outcomes.

In conclusion, the completion of UX research and persona development has been instrumental in shaping the design and implementation of effective cybersecurity education tools for high schools in Poland and the Czech Republic. By focusing on user needs and preferences, we have created solutions that are not only technologically robust but also intuitive and user-centric, thereby maximizing their impact on educational outcomes

06

SUMMARIZING THE OPERATION OF  
THE CYBERSEC EDUCHECK  
PROJECT IN PHASE REPORT

## II. Summary of the course of activities

### 02. School Recruitment Process

The recruitment of schools for the project was conducted collaboratively by Coventry University and partner in Czechia. This involved direct contact with schools that were already engaged with cybersecurity initiatives or showed interest in enhancing their cybersecurity education.

In Poland, a significant number of the recruited schools were private institutions, which demonstrated a greater willingness to participate in additional activities and pilot programs. The recruitment process began in March and concluded by the end of April. Following the successful recruitment, an introductory event was organized in April to familiarize the participating schools with the project's objectives, methodologies, and expected outcomes and offering additional knowledge. This event served as a platform for educators to exchange ideas and set the stage for a productive collaboration throughout the project's duration.





## List of schools and research participants:

In Poland, 17 teachers and 443 students participated in the survey, whereas in the Czechia, 5 teachers and 198 students took part.

### POLAND:

#### Teachers:

- Navigo: 5 pax
- Liceum Przyszłości: 7 pax
- LO X: 1 pax
- BISC Wrocław: 2 pax
- IPS Wrocław: 2 pax

#### Students:

- Navigo: 26 pax
- LO X: 385 pax
- Liceum Przyszłości: 28 pax
- BISC Wrocław: 2 pax
- Other: 2 pax



### CZECHIA:

#### Teachers:

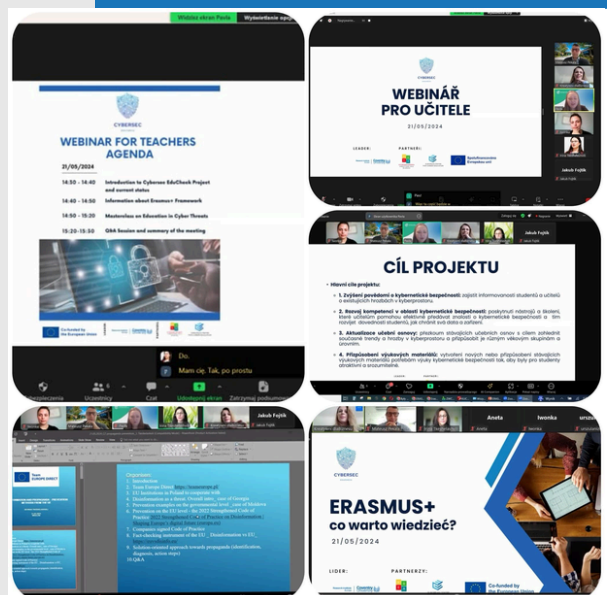
- Střední škola technická a ekonomická: 1 pax
- Gymnázium Duhovka: 1 pax
- Gymnázium: 1 pax
- Gymnázium Karla Sladkovského: 1 pax
- Hotelová škola: 1 pax

#### Students:

- Střední škola technická a ekonomická: 64 pax
- Gymnázium Duhovka: 35 pax
- Gymnázium: 53 pax
- Gymnázium Karla Sladkovského: 24 pax
- Hotelová škola: 22 pax

## II. Summary of the course of activities

### 03. Webinar for teachers under research



On 21st May 2024 a webinar on cyber threats was organized for the teachers in Poland and Czechia who participated in the project. It was moderated by our experts, Mateusz Pekala and Pavla Vybihalova, who introduced the audience with the goals and merits of the project, as well as the Erasmus+ programme.

## WEBINAR FOR TEACHERS

The teachers had an opportunity to participate in a workshop moderated by Irina Tkeshelashvili, a member of Team Europe Direct Poland, which constitutes a panel of the European Commission experts on international politics and relations. She gave an interesting speech about the importance of cyber awareness in the educational context, based on her experience on international markets, such as Georgia.



CYBERSEC  
EDUCHECK

## WEBINAR FOR TEACHERS AGENDA

21/05/2024

- |               |   |
|---------------|---|
| 14:30 - 14:40 | <b>Introduction to Cybersec EduCheck Project and current status</b> |
| 14:40 - 14:50 | <b>Information about Erasmus+ Framework</b>                         |
| 14:50 - 15:20 | <b>Masterclass on Education in Cyber Threats</b>                    |
| 15:20-15:30   | <b>Q&amp;A Session and summary of the meeting</b>                   |



Co-funded by  
the European Union

LEADER:

Research Institute Europe

Coventry University

PARTNER:

SPOTKANIE KREATYWNOSTY DLA BUDUCI

EUROPEAN CENTRE FOR CAREER EDUCATION

## II. Summary of the course of activities

### 04. Research Activities



#### Surveys

- **High School Students:** Surveys were distributed to 443 students in Poland and 198 students in the Czech Republic. The surveys focused on assessing students' awareness of cybersecurity threats, identifying knowledge gaps, and evaluating the effectiveness of existing educational methods.
- **Teachers:** Surveys were completed by 17 teachers in Poland and 5 teachers in the Czech Republic. These surveys aimed to gauge teachers' perspectives on their role in cybersecurity education, the challenges they face, and their suggestions for improvement.

#### Students from Poland

443

Surveys were distributed to 443 students in Poland.

#### Students from Czech

198

Surveys were distributed to 198 students in the Czech Republic.

#### Teachers

22

Surveys were completed by 17 teachers in Poland and 5 teachers in the Czech Republic.



## II. Summary of the course of activities

### 04. Research Activities



#### Interviews:

- Teachers: Interviews were conducted with 8 teachers (3 in Poland and 5 in the Czech Republic) to explore their views on students' cybersecurity needs, the efficacy of current teaching methods, and their suggestions for enhancing cybersecurity education.

8

#### Teachers

Interviews were conducted with 8 teachers (3 in Poland and 5 in the Czech Republic)

## II. Summary of the course of activities

### 05. Key Findings From Research

This part synthesizes key findings from research on cybersecurity education practices in high schools, based on responses gathered from educators. The findings highlight various methods, challenges, and effective strategies observed in teaching cybersecurity to students.

The assessment of high school students' cybersecurity awareness reveals significant disparities between self-assessment and external evaluation. While students rate themselves highly at 3.89 out of 5 in cybersecurity awareness, teachers rate them lower at 2.86. This indicates a perception gap that suggests a need for more comprehensive education on cybersecurity practices, especially advanced measures like Multi-Factor Authentication (MFA), which half of the students are unfamiliar with.

The survey also highlights concerning trends in internet usage and habits among students. A majority, 61%, spend 4 hours or more online daily, often checking devices before sleep, potentially affecting sleep quality and overall well-being.

Regarding online safety, 25% of respondents reported experiencing cyberbullying or online hate, while 60% did not, and others chose not to answer, underscoring the sensitivity of the issue. Responses varied in how incidents were handled, with a significant number choosing to ignore or do nothing (72), while others responded negatively (24) or attempted to help or report (13).

Students expressed varied ideas on improving cybersecurity awareness, including specific topics they feel should be included in cybersecurity classes. These range from addressing cyberbullying and specific threats to general cybersecurity education and mixed topics.

Open-ended responses also revealed a diversity of opinions. Many responses lacked relevance or were negative, while others offered constructive feedback on topics like browser security. Some respondents shared personal experiences with cyberbullying and emphasized the need for better protective measures and stricter online regulations for young users.

Overall, while students demonstrate a reasonable level of self-awareness in cybersecurity, there is a clear opportunity to enhance education around advanced security measures and address prevalent issues like cyberbullying more effectively.



#### INTERNET

61%, spend 4 hours or more online daily usage internet.



#### ONLINE SAFETY

25% of respondents reported experiencing cyberbullying or online hate.



#### CYBERSECURITY AWARENESS

Students rate themselves highly at 3.89 out of 5 in cybersecurity awareness.



#### CYBERSECURITY PRACTICES

Indicates a perception gap suggests a need for more comprehensive education on cybersecurity.



## Effective cybersecurity education

”

Effective cybersecurity education in high schools requires a balanced approach that combines traditional teaching methods with interactive and practical learning experiences.

### Current Awareness and Knowledge Gaps:

High school students demonstrate a general awareness of cybersecurity threats such as cyberbullying, privacy issues, phishing, and identity theft. They are familiar with basic concepts like online privacy and the risks of sharing personal information. However, their understanding often lacks depth, leading them to underestimate the complexity and prevalence of these threats. For instance, students know about the dangers of weak passwords and the need for secure browsing but frequently fail to apply this knowledge consistently in their online behaviors.

Students show significant gaps in their cybersecurity knowledge, particularly in practical measures. Many do not understand how to create strong, unique passwords or the importance of two-factor authentication. They also struggle to verify the credibility of websites and discern between legitimate and fake news sources. This lack of critical evaluation skills makes them vulnerable to misinformation and phishing attacks. Additionally, students often do not fully grasp the potential long-term consequences of their online actions, such as data theft and unauthorized data sharing.

### Beliefs, Concerns, and Educational Effectiveness:

High school students harbor various fears and beliefs that influence their attitudes and behaviors regarding technology use. They are concerned about identity theft, privacy breaches, and the impact of cyberbullying on their social lives. Despite these concerns, many students believe they can manage these risks on their own, leading to inconsistent application of safety practices. This belief sometimes results in a false sense of security, where they feel immune to cyber threats until they experience an incident firsthand. The fear of privacy invasion and exposure to harmful content also shapes their cautious approach to online interactions.





Effective cybersecurity education in high schools requires a balanced approach that combines traditional teaching methods with interactive and practical learning experiences. Traditional teaching approaches, such as lectures, are universally employed for imparting theoretical cybersecurity knowledge. However, interactive learning methods such as group discussions, case studies, and role-playing are favored for their ability to engage students and apply cybersecurity concepts to real-world scenarios. Practical exercises and simulations are particularly valued for providing hands-on experience and demonstrating the consequences of cyber threats. Personal anecdotes and real-life examples resonate strongly with students, making abstract concepts more relatable and impactful. The use of online tools like "haveibeenpwned" to check for potential data breaches has created significant awareness among students about the vulnerability of their personal information. Group projects and collaborative learning activities, such as "Stop Cyberbullying" campaigns and group-based assignments, foster teamwork and allow students to explore cybersecurity issues in depth. These methods not only engage students but also enhance their practical skills and knowledge.

## **The Role of School Staff:**

Secondary school staff, including teachers and principals, acknowledge their crucial role in shaping students' cybersecurity competencies but face significant challenges. These challenges include a lack of up-to-date teaching materials, limited time for dedicated cybersecurity education, and uncertainty about their own cybersecurity knowledge. Many educators express a need for more training and resources to effectively teach cybersecurity. They also see the potential for improvement through better integration of cybersecurity topics across the curriculum and increased involvement of external experts. Encouraging a school-wide culture of cybersecurity awareness and promoting good practices are seen as key steps towards enhancing students' safe use of technology.

## II. Summary of the course of activities

### 06. Teaching Opportunities

Teachers have observed a range of cyber behaviors and threats encountered by students, providing insight into both the nature of these threats and how students attempt to manage them. One prevalent issue is cyberbullying, where students often face humiliation, exclusion, criticism, and manipulation of images or videos. While they tend to report such incidents to teachers or parents, especially when school community members are involved, many initially try to handle these situations on their own using various strategies.

Privacy issues are another significant concern, with students frequently sharing personal and sensitive information online, including through public social media accounts like Instagram. Despite an awareness that the internet is not anonymous, students struggle to protect their privacy, leading to risks such as data theft, unauthorized data sharing, and exposure to harmful content.



Phishing and data theft are widespread threats that students often fall victim to due to a lack of sufficient cybersecurity knowledge. Common preventive measures suggested include two-factor authentication, verifying website credibility, and avoiding unknown links. Additionally, students exhibit inadequate cybersecurity practices by using weak and repetitive passwords, sharing passwords with others, and failing to log out from private accounts, making them vulnerable to unauthorized account access and identity theft.

The struggle to identify legitimate sources and differentiate between factual and fake information is another challenge. Students often treat social media information as factual and have difficulty critically evaluating online content, leading to the spread of misinformation and manipulation.

## II. Summary of the course of activities

### 06. Teaching Opportunities

Excessive internet use and exposure to harmful content, such as violence and pornography, are also noted. Students spend excessive time online, often accessing inappropriate content and failing to self-regulate. This overuse is linked to the pursuit of unrealistic standards of appearance and behavior.



Finally, there is a general lack of cybersecurity awareness among students. They have limited knowledge about cybersecurity measures and the potential consequences of their online actions, making them susceptible to manipulation, privacy breaches, and exploitation.





Teachers face several challenges in delivering effective cybersecurity education. Educators often struggle with ensuring student engagement and the perception of cybersecurity's importance, as students may trivialize the issues or fail to apply theoretical knowledge practically. Resource constraints, such as a lack of adequate teaching materials, time, uncertainty about personal knowledge sufficiency, and insufficient access to equipment, hinder effective teaching. Additionally, some schools struggle with integrating cybersecurity comprehensively into the curriculum and raising awareness about its importance.




To address these challenges, several effective strategies and tools have been identified. Inviting cybersecurity experts to discuss current issues and real-life scenarios enhances learning and relevance. Utilizing interactive methods like surveys, discussions, and brainstorming sessions fosters student engagement and deeper understanding. Practical applications, including hands-on activities, projects, and simulations, effectively bridge theoretical knowledge with real-world application. Access to comprehensive educational resources, including textbooks, dedicated training sessions, and online tools, supports effective cybersecurity education. Promoting good practices, such as sharing knowledge within the school community and involving parents, can enhance the overall effectiveness of cybersecurity education. Providing clear incident response protocols and fostering interdisciplinary collaboration also contribute to a more cohesive and impactful learning experience.

Effective cybersecurity education in high schools requires a balanced approach that combines traditional teaching methods with interactive and practical learning experiences. Educators play a crucial role in overcoming challenges by leveraging innovative teaching strategies, involving experts, and providing ample opportunities for students to apply their knowledge practically. Addressing resource constraints and enhancing integration across the curriculum are essential for fostering a cybersecurity-aware generation equipped to navigate digital environments safely.

# More information about project



**CYBERSEC**  
EDUCHECK

-  <https://www.coventry.ac.uk/wroclaw/>
-  <https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/>
-  <https://eccedu.net/>

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

All results developed within the framework of this project are made available under open licenses (CC BY-NC 4.0). They can be used free of charge and without restrictions. Copying or processing these materials in whole or in part without the author's permission is prohibited. If the results are used, it is necessary to mention the source of funding and its authors.

PROJECT NO. 2023-2-PL01-KA210-VET-000176822



Co-funded by  
the European Union

LEADER:

Research Institute  
Europe

Coventry  
University

PARTNERS:

K R  
E A  
STOWARZYSZENIE  
KREATYWNI DLA  
BIZNESU

EUROPEAN CENTRE  
FOR CAREER EDUCATION