



SuperCyberKids

Teacher Training – English Version
General introduction to Cybersecurity Education



Co-funded by
the European Union

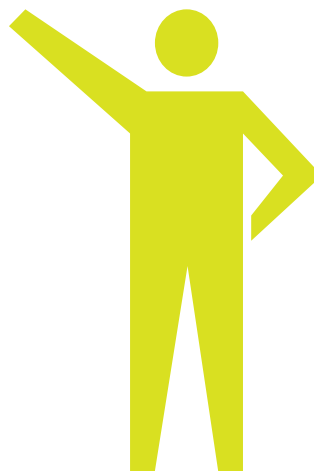
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for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

Cybersecurity for kids, why should we care?

97%

of young people in the EU use the internet
daily (EUROSTAT)

Cybercrime's economic
impact is equivalent to the
GDP of Spain



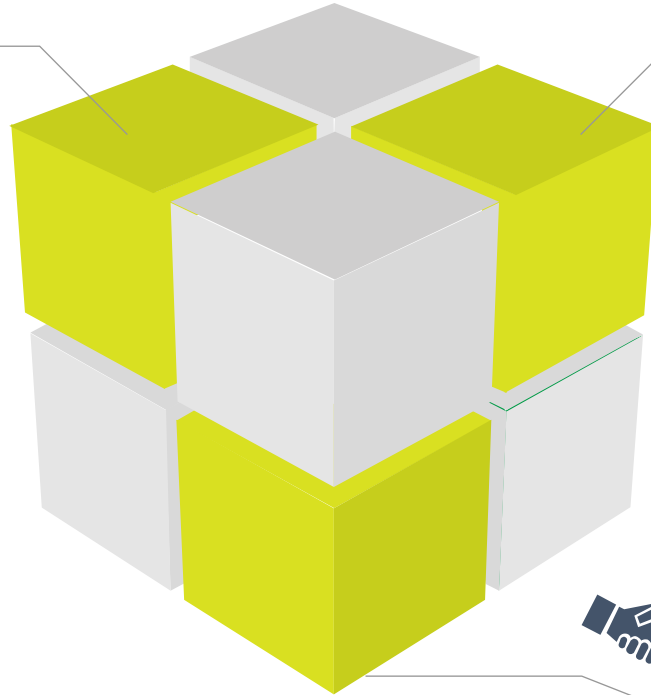
72%

of children globally have experienced at least one
type of cyber threat online (Global Cybersecurity
Forum)

Cybersecurity for kids, why should we care?

ENISA Threat Landscape

ENISA's Threat Landscape report for 2023 identified eight key threats of which phishing and social engineering attacks are the most likely to target children directly.



Initiatives to raise awareness and increase skills

Initiatives to raise awareness and increase the skills of kids in cybersecurity are crucial for their future as adults but also as citizens, adding another lifelong learning dimension to education.

- Most education efforts have focused on students in high school or above and have involved a wide variety of approaches.
- SuperCyberKids aims to fill the skills and awareness gap among kids aged from 8 to 13 years.



Collaborations

Cybersecurity is no longer just the responsibility of technical experts; it's a societal responsibility, especially for schools. Cyberspace is the largest shared space in human history, and educators, including parents, play a key role in keeping it safe.

- Social engineering attacks are a broad group of attacks in which there is an attempt to manipulate the user.
- The user can be manipulated into taking an action through four different mechanisms:

Offers of Money

Example: you have just one chance to earn 1,000 euro click here to collect

Ideology of the user

Example: sign this online petition to stop animal testing

Threats

Example: we have already hacked your webcam and recorded you watching things you shouldn't

Ego stroking

Example: we would like to recognise your work for charity click the link below

A phishing attack is a specific example of a social engineering attack.

- Fake emails that trick kids into downloading malware or giving away personal info.
- The 2023 ENISA report highlights a rise in "phishing as a service," allowing cybercriminals to pay for software to launch attacks, leading to more phishing and scams.

Fake
News

Phishing

Fake News

- Fake news and online scams targeting children, often on social media platforms like TikTok and Instagram.
- Example Disinformation: In October 2023, thousands of establishments in Estonia received bomb threats, including schools. There was also additional information shared on Snapchat and TikTok about how some schools had already been blown up. None of this happened.

Why might children be targeted?



Children are often targeted through shared family devices, which can unknowingly download malware. Poor cyber hygiene, such as reusing passwords, increases the risk. They may also accidentally share personal information or access parents' credit card details, making them vulnerable to phishing and blackmail. Educating everyone on cyber hygiene is key to preventing these attacks.

Cybercriminals may target children for exploitation or to spy on them. Children are vulnerable due to limited technological knowledge and lack of awareness about the impact of their actions, such as hacking or sharing personal content. These issues highlight the need for both cyber hygiene and a broader understanding of online ethics and legal consequences.

Loss of accounts

- Cybercriminals use phishing to access children's gaming accounts and steal or sell virtual items. All accounts are at risk, even if they don't have valuable items, as hackers target them indiscriminately.

Low level ransom-ware attacks

- While high-level ransomware attacks typically target organizations, children may be vulnerable to ransomware in online games, where their virtual property can be stolen or held for ransom. Students should be aware of this risk and practice good cyber hygiene.

Loot boxes and gambling targeting children

- Children are increasingly targeted by online activities that aren't illegal but can still cause harm. Microtransactions in free games encourage spending small amounts of money, often without realizing the total cost.
- Loot boxes, a form of in-game gambling, are also rising, where players may win valuable items or nothing at all. Both issues highlight the need for cyber hygiene education to help children understand these risks.

01

Cyber education must raise awareness of dangers without encouraging children to experiment with harmful tools, similar to how drug education informs without promoting use.

02

Some believe children can't be effective hackers, but this is false. Beginner hackers, or "script kiddies," use online code to cause damage without fully understanding it. Basic coding skills, like installing mods or following instructions, can enable these attacks.

03

Cybersecurity education should teach both defense and ethical guidelines, helping kids understand legal boundaries and redirecting their curiosity toward positive cybersecurity pursuits.



Why should schools care?



Cybersecurity education for children aged 8-13 is becoming increasingly important due to the growing complexity of digital threats. Integrating cybersecurity topics into existing subjects like IT, Computer Science, and General Studies ensures students learn key concepts without overhauling the curriculum. Additionally, accessible online resources, such as courses and games, extend learning beyond the classroom, catering to diverse student needs.



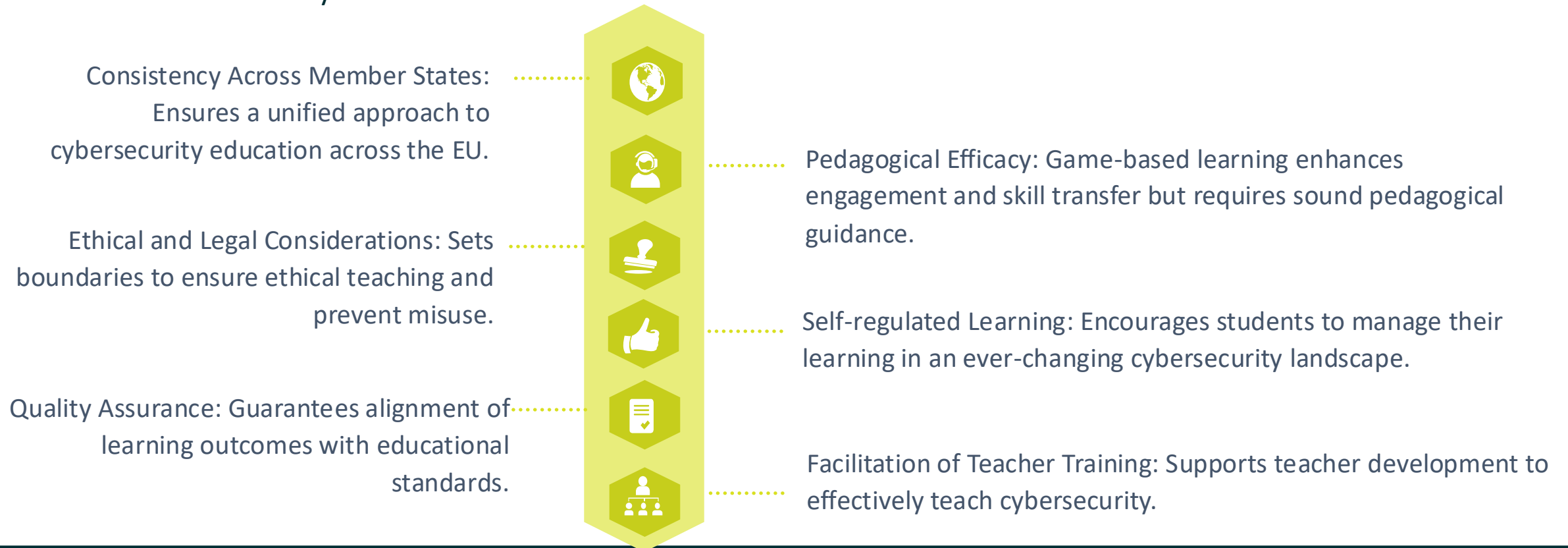
Co-funded by
the European Union

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 the granting authority can be held responsible for them.



The Need for a Unified EU Framework

- The introduction of Cybersecurity Education for children aged 8-13 requires a standardized EU framework, like the SuperCyberKids project, which integrates game-based learning into existing curricula with guidelines for educators. Key benefits include:





SuperCyberKids is here to help



SuperCyberKids resource search

To facilitate exploration of the ontology, a prototype online tool has been produced that allows step-by-step navigation of the elements and relations the ontology expresses. [Click here](#) to access the online prototype tool.

Age

Language

Domain

Competencies

Type of resource

Smart search

All

All

All

All

All

Cyber

Search

The following SCK-approved items may be useful to you:

Basics of Cybersecurity

Level: **Core**

Lorem ipsum dolor sit amet consectetur. Magna vestibulum accumsan ornare quam facilis dictum egestas. Massa proin donec pharetra viverra. Eu velit senectus in ut.

Competencies

Cyber bullying

Level: **Advanced**

Lorem ipsum dolor sit amet consectetur. Magna vestibulum accumsan ornare quam facilis dictum egestas. Massa proin donec pharetra viverra. Eu velit senectus in ut.

Competencies

Items suggested by the SCK Community

Finance in the Cyber age

★ ★ ★ ★ ★ 5.0 Age: 10-13

Lorem ipsum dolor sit amet consectetur. Magna vestibulum accumsan ornare quam facilis dictum egestas. Massa proin donec pharetra viverra. Eu velit senectus in ut.

YouTube videos

Competencies

george-green

Deep dive: Cybersecurity

★ ★ ★ ★ ★ 5.0 Age: 10-13

Lorem ipsum dolor sit amet consectetur. Magna vestibulum accumsan ornare quam facilis dictum egestas. Massa proin donec pharetra viverra. Eu velit senectus in ut.

PDF document

Competencies

Malicious Code

Understand Content safety

Understand Basic Cyber Threats

Use strategies to protect against cyber attackers

terryturquoise

SuperCyberDataSaver!

★ ★ ★ ★ ★ 5.0 Age: 8-9

Lorem ipsum dolor sit amet consectetur. Magna vestibulum accumsan ornare quam facilis dictum egestas. Massa proin donec pharetra viverra. Eu velit senectus in ut.

Videogame

Competencies

bianca.blue

Your data in the cyber world

★ ★ ★ ★ ★ 5.0 Age: 8-9

Lorem ipsum dolor sit amet consectetur. Magna vestibulum accumsan ornare quam facilis dictum egestas. Massa proin donec pharetra viverra. Eu velit senectus in ut.

PDF document

Competencies

TheBruceBrown

Co-funded by
the European Union

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 the granting authority can be held responsible for them.