2025

#24

HEADSTART

CYBERSECURITY EDUCATION IN SCHOOL

BY LUCA LASZLO AND THE SUPERCYBERKIDS TEAM

This HeadStart offers practical guidance and resources for planning and implementing cybersecurity education, ensuring pupils gain the skills they need to navigate the digital world safely.

This card will help you answer questions such as:

- How can I ensure students develop strong cybersecurity skills throughout their school careers?
- How can I prepare staff to deliver and support this learning effectively?
- How can I engage parents and carers, so they reinforce these skills at home?
- What practical resources and tools can I use in the classroom?

WHAT IS CYBERSECURITY EDUCATION & WHY DOES IT MATTER?

Cybersecurity education teaches children how to protect themselves and their devices online. It covers topics such as privacy, online behaviour, malware awareness, and device safety – fundamental skills in today's digitally connected world.

WHY SHOULD IT BE TAUGHT IN SCHOOLS?

Children are active online from an early age, often before they fully understand the risks. Schools play a vital role in ensuring all pupils receive consistent, age-appropriate guidance, rather than relying solely on uneven learning at home. Early, structured education builds lifelong habits of safe and responsible digital participation.

HOW CAN I ENSURE STUDENTS DEVELOP STRONG CYBERSECURITY SKILLS THROUGHOUT THEIR SCHOOL CAREERS?

It is important to make cybersecurity a clear and measurable part of the curriculum from the earliest years. Set age-appropriate learning objectives that help children recognise online risks and scams, protect their personal information and privacy, communicate safely and respectfully, and build positive, healthy habits when interacting online. As students grow older, they should also understand that they can be potential perpetrators of unsafe or harmful online behaviour, and the consequences of such actions must be made clear. These skills should not be taught only in ICT lessons but integrated across subjects and reinforced each year so that pupils' knowledge develops progressively. Using interactive, problem-solving activities will further strengthen students' confidence and help them build lasting habits that support safe and responsible online engagement.

HOW CAN I PREPARE STAFF TO DELIVER AND SUPPORT THIS LEARNING EFFECTIVELY?

To prepare staff to deliver and support cybersecurity learning effectively, schools should provide professional development that builds teachers' confidence both in the subject matter and in how to teach it. This can include training sessions on core cybersecurity concepts as well as practical classroom strategies. Teachers benefit from having ready-to-use resources, lesson plans, and activities from trusted educational initiatives such as SuperCyberKids, which can make it easier to embed learning into their daily practice. It is also valuable to identify a staff member or small team to lead on digital safety, coordinate resources, and mentor colleagues. Creating opportunities for teachers to share experiences

and adapt strategies to different age groups and learning needs further strengthens their capacity. When staff feel equipped and supported in this way, cybersecurity education becomes a routine and integrated part of teaching across the school.

HOW CAN I ENGAGE PARENTS AND CARERS, SO THEY REINFORCE THESE SKILLS AT HOME?

Engaging parents and carers is essential to ensure that the cybersecurity skills pupils learn at school are reinforced at home. Strong home–school cooperation helps deliver consistent messages and behaviours. Schools can hold parent information evenings or workshops to demonstrate the same tools and games pupils use in class, such as *Spoofy*, *Nabbovaldo*, and *The Cyber Blackmail*. Providing take-home guides with clear tips for safe online behaviour gives families practical support, while encouraging parents to talk regularly with their children about online activities and choices helps keep communication open. Updates shared through newsletters, the school website, or parent–teacher meetings also keep the topic visible. By framing the conversation around empowerment —helping children make wise choices — schools can motivate parents to participate actively, leading to stronger and more positive outcomes.

WHAT PRACTICAL RESOURCES AND TOOLS CAN I USE IN THE CLASSROOM?

It is most effective to use resources that are interactive, engaging, and adaptable for different age groups. For younger students, the game *Spoofy* introduces safe online behaviour through scenarios and problem-solving activities. Older pupils can explore *Nabbovaldo*, a game set in the fictional city of Internetopolis, which teaches good practices around cybersecurity. Teachers can also draw on lesson plans, activity sheets, and handbooks from initiatives like SuperCyberKids to support structured learning. Roleplay exercises and discussions about real-life scenarios pupils may encounter online are another powerful way to help them apply knowledge in practical situations. By selecting free, accessible, and engaging resources, schools can embed cybersecurity education effectively without adding unnecessary strain on budgets, staff workload, or coordinators. Cybersecurity education does not need to be limited to computer science courses; it can be effectively integrated across the curriculum to build digital awareness and resilience in students. In language arts, for example, students can strengthen literacy and critical thinking skills by evaluating the credibility of online information or debating issues such as privacy and online safety. Mathematics classes can introduce foundational ideas like cryptography and data analysis through activities that connect directly to cybersecurity concepts, while social studies courses can explore the role of cyberattacks in global events, the ethics of surveillance, and the history of digital technologies. Embedding these themes in existing subjects makes cybersecurity relevant to all learners, not just those pursuing technology pathways.

Science, arts, and career-focused subjects also offer natural opportunities to weave in cybersecurity education. Biology and environmental science can highlight the parallels between digital and biological systems, such as the spread of viruses or the protection of critical infrastructure like power grids. Visual and performing arts can engage students in creating campaigns, skits, or digital media that promote safe online practices. In career and technical education, students can learn how cybersecurity shapes fields such as healthcare, business, and finance, ensuring they are prepared for the expectations of the modern workforce.

For further information, visit the website of the SuperCyberKids project, where you will find more guidance on how to implement cybersecurity education in practice, what the necessary skills and competences children should have are, and classroom-ready resources: [supercyberkids.eu]