2025

#23

HEADSTART

CYBERSECURITY IN SCHOOL

BY LUCA LASZLO AND THE SUPERCYBERKIDS TEAM

 # This card provides tools for practical questions like:

- How to minimize the effects of cyberattacks?
- What are the most critical steps to mitigate effects of cyberattacks on my school?
- How can I prepare the school community for cyberattacks?
- What should I do if my school is attacked?

WHAT IS CYBERSECURITY?

Cybersecurity is the set of practices and measures that protect your school's digital systems, data, and networks from theft, damage, or disruption. In schools, it safeguards student and staff personal data, financial systems, teaching resources, and communication tools from unauthorized access and misuse.

Cybersecurity at school is a leadership responsibility. By prioritising prevention, preparing the school community, and responding effectively when incidents occur, you can protect your school's learning environment, and strengthen the trust and wellbeing of students, parents, and staff.

In today's turbulent digital world, we all know only too well what can happen if we let down our guard. And schools are certainly no exception.

HOW TO MINIMIZE THE EFFECTS OF CYBERATTACKS?

Cyberattacks happen every 13 seconds around the world, so it is near impossible to completely avoid them. However, you can mitigate the impact.

Cybersecurity is a series of processes that must be done consistently and regularly with checks to ensure that the steps are being followed.

As a first step, make sure that you are familiar with the national, regional and local regulations of cybersecurity in schools, and the mandatory steps you need to take as required by law.

- **Establish clear policies** for password management, device use, and data access.
- **Use strong authentication** for all staff and administrative accounts. Consider the use of two factor authentication for access.
- **Limit access rights** so staff and students only have access to what they need.
- **Keep software updated** on all school devices, including those used remotely. This limits the possible avenues for viruses to be introduced to the school system. It is strongly advised to not use personal devices for schoolwork and accounts, not just in school, but at all.
- **Secure your network** with firewalls, filtering, and encryption. Use a reliable vendor to keep these up to date or have a schedule for them to be updated and follow it.
- **Back up critical data** regularly and securely – store a copy offline, or use a reliable cloud-based storage solution.
- **Be aware of possible fake threats and misinformation** strategies that could cause disruption and anxiety in the school.

What are the most critical steps to reduce the impact and mitigate effects of cyberattacks on my school?

- **Have all staff and students trained** to spot suspicious emails, links, and chat requests. Remember phishing scams leverage four basic elements to attack 1) fear of repercussions, 2) time urgency, 3) financial peril, and 4) verification difficulty.
- **Update and patch systems** as soon as security fixes are available. This will help to limit technical exploits that can gain access to your system.

- **Restrict use of personal devices** on school networks without security checks. This reduces the risk of viruses spreading and malware from being introduced.
- **Monitor network activity** for unusual patterns. Has there been a sudden spike in the amount of data that has been downloaded, is there heavy traffic on the system after school hours or during holidays?
- **Perform regular audits**: send a scheduled reminder for staff and students to change their emails or require them to use a new strong email every new semester. Check that the policies you have in place are being followed. Check that all devices on the network have been updated.
- **Test your defences** through regular security audits or penetration testing, including regular phishing campaigns. Keep in mind that this will have a significant monetary cost.
- Have a safe method for students to report security exploits they have discovered. Your students are going to look for exploits more so if they are told not to.
- Ensure physical security as well. Make sure the school's different devices are secured and not easily accessible to strangers or other unwanted parties.

How can I prepare the school community for cyberattacks?

- **Build awareness**: Include cybersecurity awareness in staff meetings and student assemblies. Be aware of the potential consequences of a data breach. It can lead to a lawsuit or EU fines.
- **Develop an incident response plan** with clear steps for detection, reporting, containment, and recovery.
- **Assign responsibilities**: Know who leads the response, who communicates with stakeholders, and who works on technical recovery.
- **Run practice scenarios** so everyone knows what to do in a crisis.
- **Create a culture of openness** so suspicious activity is reported early, without fear of blame.
- **Make sure staff is aware of who to contact outside the school,** for example the national agency that deals with cyber-attacks.
- **Integrate cybersecurity into the school curriculum** in a child appropriate way.

What immediate steps should I take if my school is attacked?

- **Isolate affected systems** to stop the spread
- **Inform your IT lead or external support team** immediately.
- **Preserve evidence** – do not delete suspicious files before investigation.
- **Notify relevant authorities.** Any attack against any school should be sent to the national agency that deals with this.
- **Communicate carefully** with staff, parents, and, where necessary, the wider public.
- **Recover from backups** once systems are secure.
- **Review and strengthen** security measures to prevent recurrence.

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]