

NaviRisk

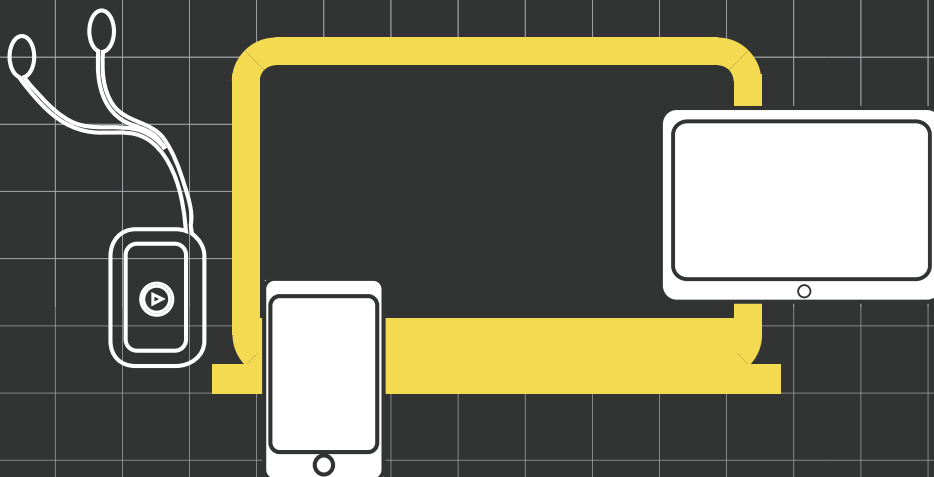
www.wearenavirisk.com

A practical guide to cyber threats
in the new school year

BACK TO SCHOOL 2023

The start of a new school year means new textbooks, friends, and safety challenges. Technology plays an increasingly important role each year in our children's lives. Therefore, when they return to school after the holidays, it is worth reminding them about potential threats and how to protect themselves against them.

Below are some main risks and practices that can help keep your child safe.



Threats in the digital and analogue world

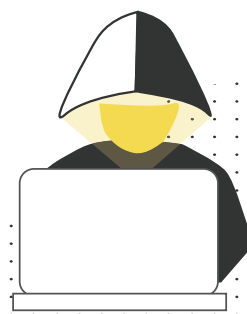


Phishing

Fraudulent e-mails or text messages that try to obtain personal information; the stolen personal information is then used by criminals to further dishonest actions against you and your children.

Cyberbullying

Children and young people are at risk of online bullying, which can severely affect their mental health. Determining the aggressor's identity can be difficult because he hides in the network.

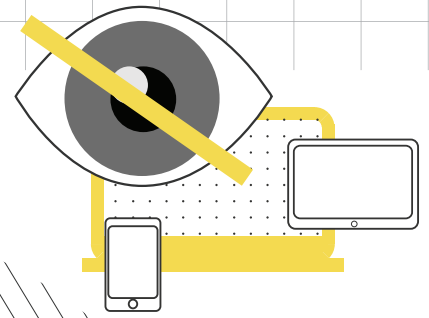


Dangerous places and people

Old school buildings or unfamiliar people in the area can be dangerous.

Inappropriate content

There is much inappropriate content circulating on the Internet that is inappropriate for younger users. The Internet facilitates access to inappropriate material.



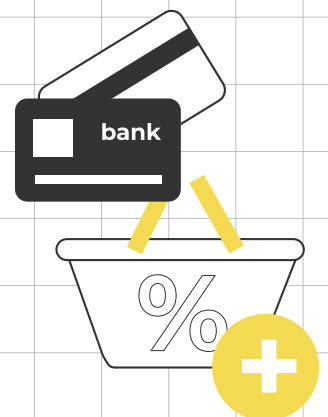
Identity and personal data theft

In both digital and analogue environments, there is a risk of data theft. This may be due to careless sharing of information online or through physical robbery, such as taking documents or credit cards. Especially at the beginning of the school year, parents and children very often fill in many forms in electronic and analogue versions, sign up for participation in many initiatives, and provide a large amount of information that should stay adequately protected. Stolen data and documents, such as school ID cards, can be used illegally.

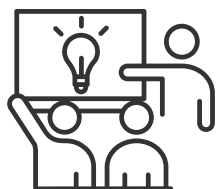
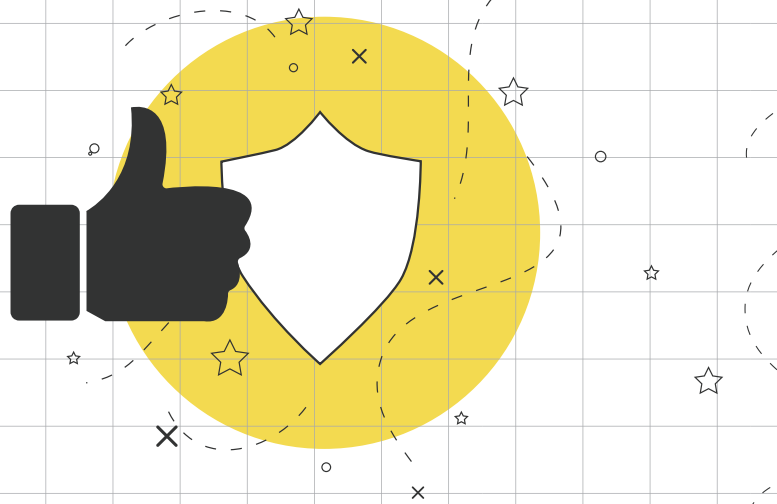


Online payments

Entering credit or debit card details on insecure sites or in response to fraudulent e-mails may lead to the theft of funds or the use of data for illegal transactions. Children may also be more susceptible to fraud in online stores that offer attractive products at too low prices.



Good practices and rules

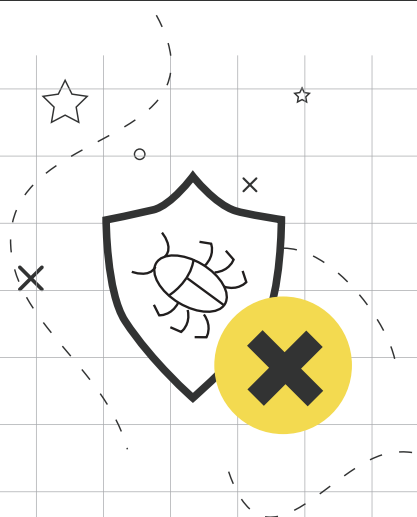


Education and Awareness

Teach yourself and your children the basics of cybersecurity. Warn children of hazards and teach them how to recognize and respond to them.

Rules for using the Internet and electronic devices

Together with your child, determine which websites and applications are safe, which applications and when they can be used.



Updates and antiviruses

Regularly update your software and use reputable antivirus programs for computers and mobile devices (tablet, smartphone).



Privacy Policies

Set appropriate privacy policies on social media profiles and other online platforms. Teach your children not to share too much personal information online



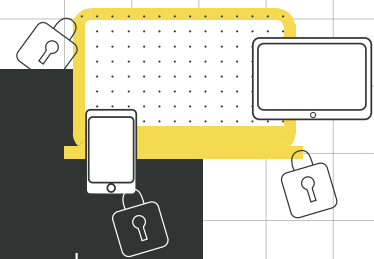
Data in the cloud

Consider what information is stored in the cloud and whether it is appropriately secured.



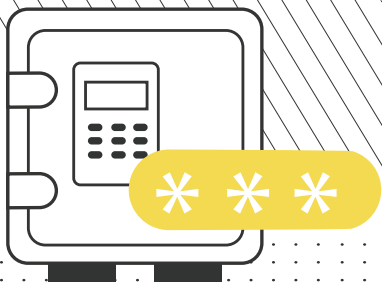
Online payments

Make sure you only use reputable websites. Never share your payment card details in response to unsolicited e-mails. Also, consider using unique prepaid cards or separate account cards for online payments with a set limit of funds that can be used for online purchases, minimizing risk.



Strong passwords

Use strong, unique passwords and safely store them - e.g. in a proven password manager. Use multi-factor authentication wherever possible.



Real-world privacy

Always keep your important documents and credit cards safe.



Keeping children safe in both the digital and analogue worlds is a task that requires the cooperation of parents, teachers and students themselves. Remember that in today's world, technology is everywhere, and while it brings many benefits, there are also risks. The key to safety is education and awareness. Teach your kids how to use technology responsibly, and they'll turn those lessons into habits that will last a lifetime.

Read more
and contact us:

www.wearenavirisk.com

 info@wearenavirisk.com