TLP: WHITE

ENSURING KIDS' ONLINE SAFETY

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS

COMMISSIONER OF COMMUNICATIONS Digital Security Authority

Co-funded by the European Union

ncc.cy

AGENDA

- Introduction
- Common Uses
- The Risks
- Controls and Safeguards
- Parents and Teachers collaboration
- Useful Information

INTRODUCTION

INTRODUCTION

Why is Cybersecurity important for our kids ?

1. Growing Online Presence: Children are spending more time online than ever before.
2. Protecting Their Future: Safe online habits start at home.
3. Stay Informed: Knowledge is the first step to prevention.

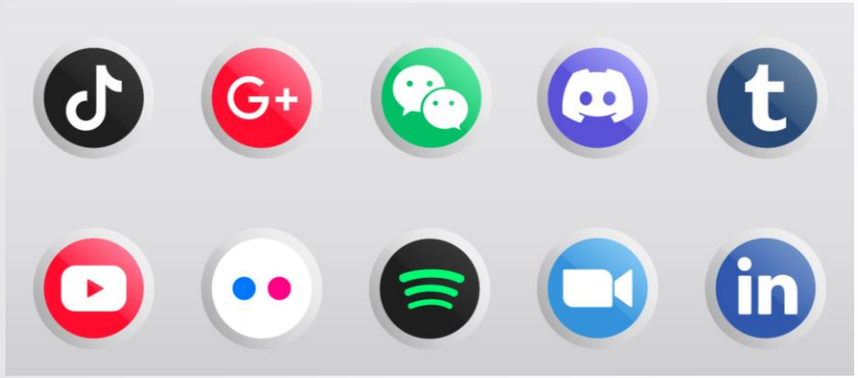
*In 2023 in the EU, **97 % of young people** used the internet daily, compared with 86 % of all individuals.***

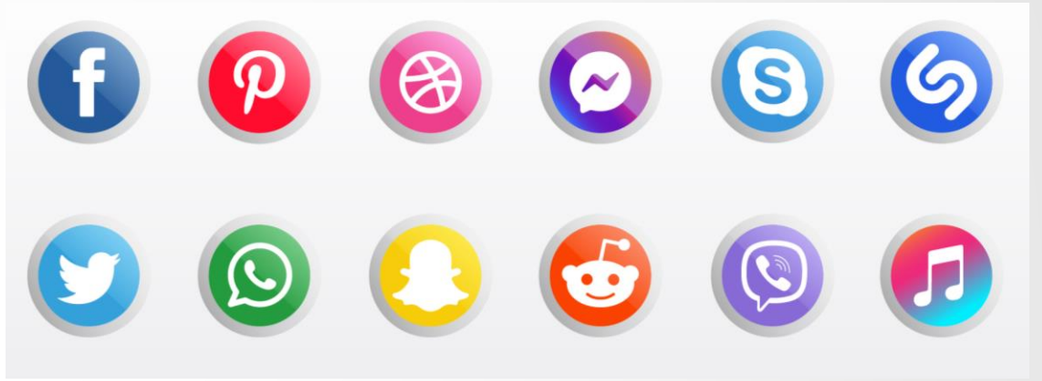
Today, we will discuss the most common used of the internet, the risks and the possible safeguards we can implement to protect them

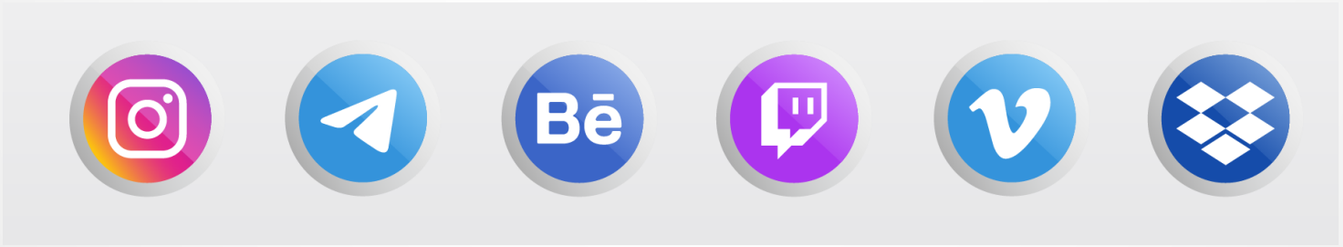
THE COMMON USES

SOCIAL MEDIA

Do you know which Social Media platforms they use ?







In 2022, 84% of young people used the internet to participate in social media networks.*

SOCIAL MEDIA

What to look out for:

- Are they sharing their personal information ?
- Who do they have in their “Friends” list ?
- Who are they chatting with ?
- Are they sharing their photos or anyone else's photos?
- Which accounts are they following ? Are these accounts appropriate for their age ?

ONLINE GAMING

- Kids are increasingly spending more and more time on online gaming platforms

- Benefits of gaming can include improved hand-eye coordination, problem-solving skills, and social connections with peers.
- But… there are also risks associated with online gaming, such as exposure to inappropriate content, cyberbullying, and potential addiction to gaming.

What to look out for:

- Age-Appropriate Games: Ensure the games are suitable for your child's age. Check ratings and reviews from credible organizations such as ESBR and PEGI. Look for the following signs

- Parental Controls: Utilize parental controls available on gaming platforms to restrict inappropriate content and manage playtime.

- Privacy Settings: Teach your child to keep personal information private. Ensure their profiles are set to private and limit the information they share.

- Secure Accounts: Use strong, unique passwords for gaming accounts and enable two-factor authentication if available.

ONLINE SHOPPING

How do kids use online shopping ?

- Buying Items: Browsing online stores for toys, clothes, or other items, often with parental supervision.
- Virtual Goods: Purchasing in-game items or digital content.

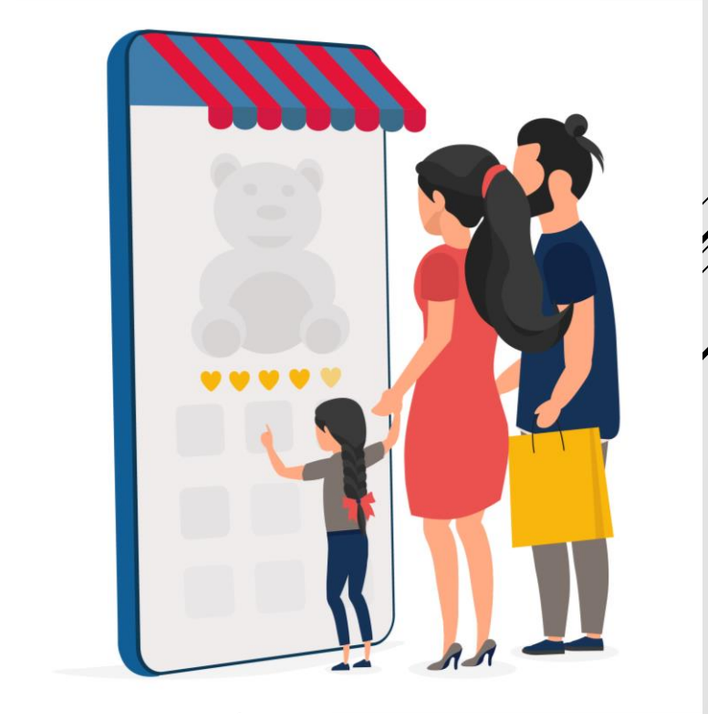
What to look out for:

Spending limits:

- Consider using prepaid cards with fixed amounts to limit spending.
- Teach kids about budgeting and the value of money.

Scams:

- Educate kids about common online scams, such as fake websites, phishing emails, and too-good-to-be-true offers.
- Encourage them to come to you if they encounter anything suspicious.
- Teach kids how to read product reviews and ratings to make informed purchasing decisions.



THE RISKS

CYBERBULLYING

What is Cyberbullying?
Cyberbullying involves using digital platforms like social media, text messages, email, and other online tools to *harass, threaten, or humiliate someone.*
It can take many forms, including spreading rumors, sharing private information without consent, sending threatening messages, and creating fake profiles to embarrass someone.

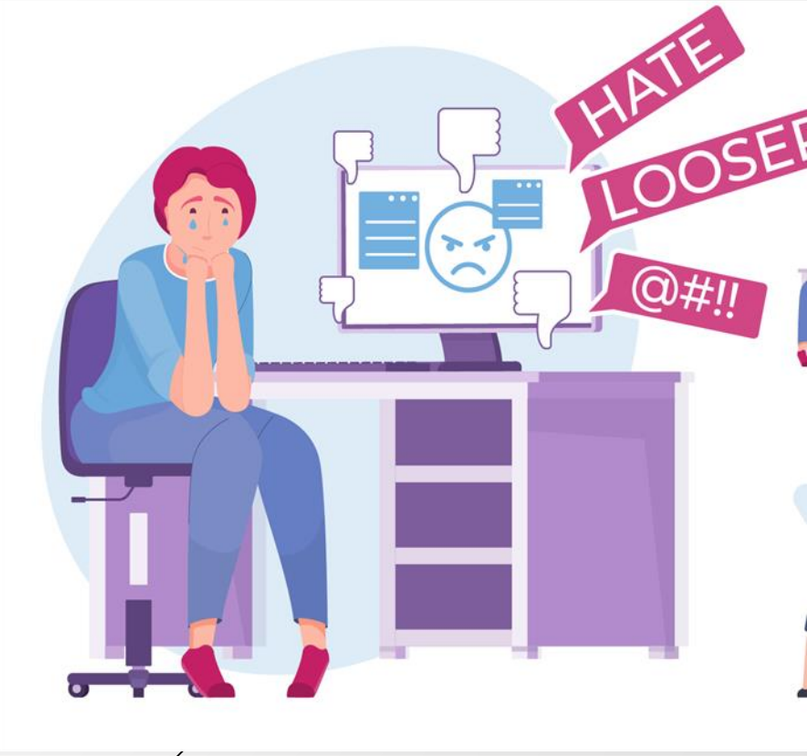
What to look out for:

- Emotional Changes: Sudden changes in mood, anxiety, depression, or irritability.
- Behavioral Changes: Reluctance to go to school, avoiding social interactions, or changes in eating and sleeping habits.
- Digital Red Flags: Unwillingness to use devices, nervousness when receiving notifications, or a sudden change in how they use their devices.

CYBERBULLYING

Responding to Cyberbullying

- Documentation: Keep records of any bullying incidents, including screenshots of messages or posts.
- Reporting: Report the bullying to the relevant platform (e.g., social media site, app) and, if necessary, to school authorities or local law enforcement.
- Support: Offer emotional support to your child and consider professional counseling if needed.



ONLINE PREDATORS

- Online Predators: These are individuals who exploit the anonymity of the internet to target, groom, and exploit children.
- Grooming Tactics: Predators may use *flattery, gifts, attention, and manipulation* to gain a child's trust and lower their defenses.
- Platforms Used: Predators can be found on social media, gaming platforms, chat rooms, and messaging apps.

INAPPROPRIATE CONTENT

Inappropriate content can have a huge impact on young individuals:

- Emotional and psychological effects: Exposure to inappropriate content can cause fear, anxiety, or desensitization to violence.
- Behavioral changes: It can influence children to mimic inappropriate behaviors.
- Addiction: Certain content, such as online pornography, can be addictive.
- Desensitization: Repeated exposure to violent or explicit content can reduce sensitivity to such material.

Inappropriate content for kids can have many types:

- Pornography and sexually explicit material
- Violence and gore
- Hate speech and discrimination
- Drug and substance abuse
- Misinformation and fake news:
- Scams and malware

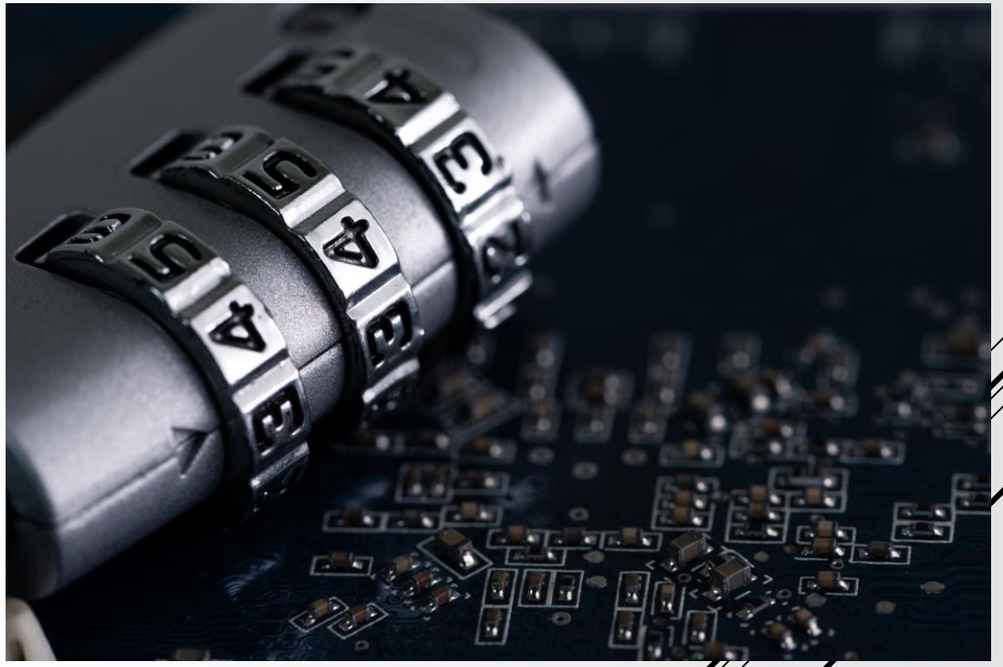
INAPPROPRIATE CONTENT

Responding after exposure:

- Stay calm: If a child encounters inappropriate content, respond calmly and avoid overreacting.
- Discuss the content: Talk about why the content is inappropriate and its potential impact.
- Reinforce safe practices: Remind children of the steps they can take to avoid similar content in the future.
- Seek professional help: If exposure has led to significant distress or behavioral changes, consider consulting a child psychologist.

PRIVACY AND IDENTITY THEFT

- Personal Information: Children's personal information, such as names, birthdates, and addresses, can be valuable to cybercriminals.
- Social Media: Social media platforms often encourage sharing personal details.
- Apps and Games: Many apps and online games collect data. Such collection is often described in the privacy policies of these apps and games.
- Data Breaches: Children’s data is often less monitored than adults', making it a target for data breaches.



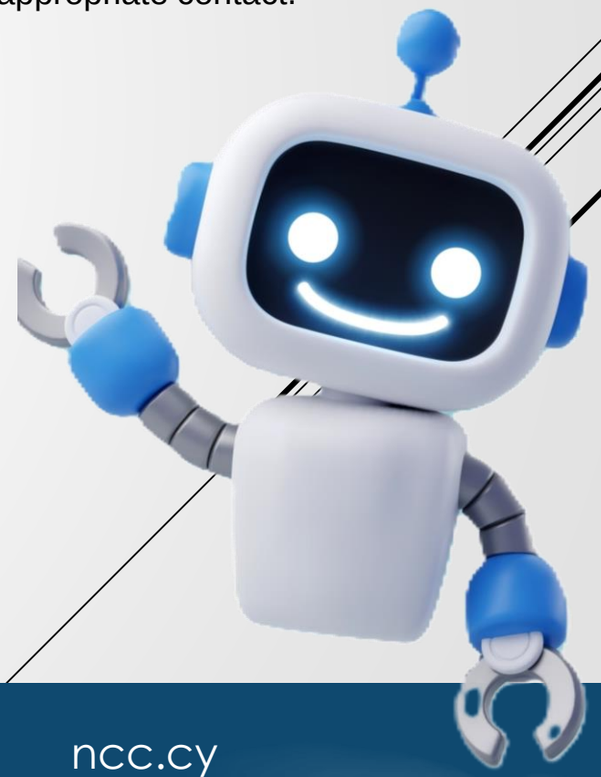
THE CONTROLS AND THE SAFEGUARDS

EDUCATION AND AWARENESS

- **Open Communication:** Foster an environment where your child feels comfortable discussing their online activities and any uncomfortable experiences.
- **Critical thinking:** Teach kids how to recognize suspicious behaviour and content.
- **Safe browsing habits**: Teach them how to recognise age-appropriate websites.
- **Online Behavior:** Teach them about the importance of not sharing personal information (like their full name, address, or school) online.
- **Recognizing Grooming:** Help them understand what grooming behavior looks like and encourage them to report any inappropriate contact.
- Make sure they know that EVERYTHING that is shared online will remain online **FOREVER**

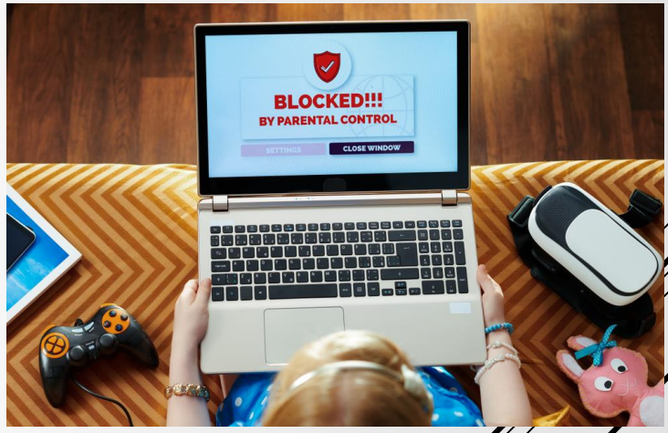
REMEMBER THOUGH! You need to keep educating yourself as well

- Stay Informed: Keep up to date with the latest trends in social media and online behavior to better understand the environments your child is navigating.
- Resources: Utilize resources from organizations like “CYberSafety” , SafeOnline and other child safety organizations to educate yourself and your child.



PARENTAL CONTROLS AND MONITORING

- **Overview of parental control tools**: Use parental control software to monitor and limit your child's online activities. Remember that some platforms have built in parental control settings (e.g. PlayStation accounts)
- **Set up filters and restrictions:** Blocking inappropriate content, limiting screen time.
- **Monitor online activity**: Regular check-ins, reviewing browser history, and using monitoring apps.
- **Privacy Settings:** Ensure that your child’s social media accounts and other online profiles are set to private.
- **Screen Time:** Set limits on the amount of time your child spends online and ensure they have a balanced lifestyle with offline activities.
- **Safe search settings:** Enable safe search settings on browsers and platforms like Google and YouTube.

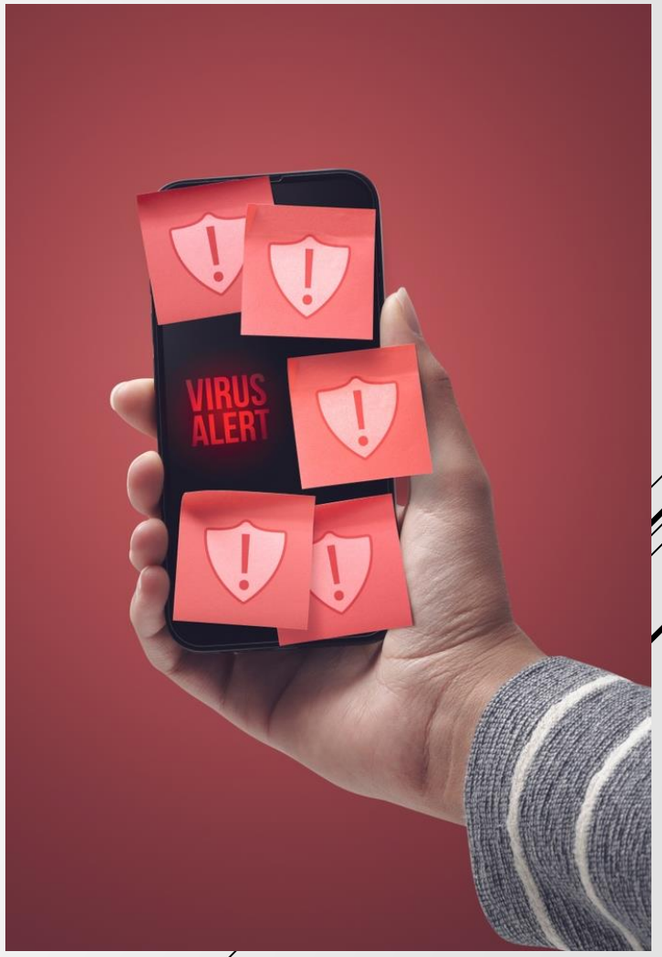


BE PROACTIVE

- **Know Their Friends:** Be aware of who your child interacts with online and encourage them to keep online friendships within their real-life social circle.
- **Regular Check-Ins:** Regularly check your child’s devices for any unfamiliar or suspicious contacts and communications.
- **Use of Technology:** Familiarize yourself with the apps and websites your child uses and understand their features and risks.

SAFE ONLINE ENVIRONMENT AT SCHOOL

- Implementing school policies: Acceptable Use Policies (AUPs) for internet use.
- Educating students: Incorporating digital literacy and online safety into the curriculum.
- Interactive Sessions: Encourage interactive sessions where children can learn about cybersecurity through games, quizzes, and practical exercises.
- Always be cautious, if you identify any signs, report it immediately
- Cybersecurity controls & measures:
  - Secure networks
  - Regular updates
  - Use of proper antivirus software
  - Filters and blacklisting/whitelisting of websites
  - Staff training

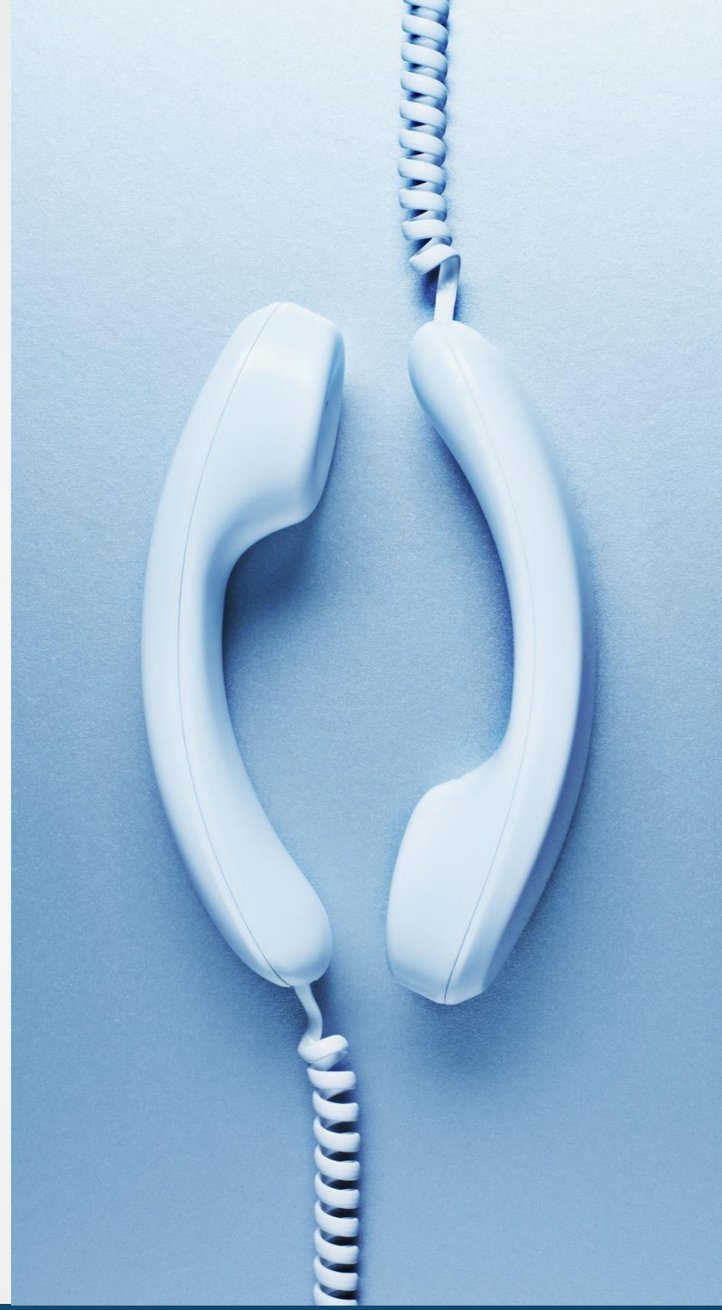


COLLABORATION BETWEEN PARENTS AND TEACHERS

COMMUNICATION

Effective communication between parents and teachers is crucial for ensuring the cybersecurity of kids.

- Regular Meetings: Schedule regular parent-teacher meetings to discuss cybersecurity issues and updates.
- Emails and Newsletters: Use emails and newsletters to keep parents informed about recent cybersecurity threats and tips.
- Online Portals: Utilize school online portals for sharing resources and updates on cybersecurity.
- Reporting mechanisms: Establishing clear processes for reporting and addressing online safety concerns with parents.



USEFUL INFORMATION

RELEVANT RESOURCES & BODIES

- National Cybersecurity Center Cyprus (NCC-CY) - https://ncc.cy/
- National CSIRT Cy - https://csirt.cy/
- Police (Cybercrime Subdivision) - https://cyberalert.cy/
- Office of the Commissioner for the protection of personal data - https://www.dataprotection.gov.cy/

- CyberSafety European Project - https://cybersafety.cy/
- Internet Safety - https://internetsafety.pi.ac.cy/


IS YOUR CHILD
SAFE ONLINE?