certSIGN

Cyber4Kids

LESSON 2.
Personal data is secret

By following these cybersecurity tips, you will become a Cyber Superhero and you will activate a magical object – The CLOAK of INVISIBILITY! This way you will be able to safely hide your secret personal data!

1 **WHAT PERSONAL DATA IS SECRET?** Never give or post on the Internet:
- your full name, date of birth, age;
- home address or the school you attend;
- phone number or email;
- details of your parents' credit cards;
- any other information about you or your family.

2 **2. HOW?** The cyber villain may ask you for this secret personal data through messages on Facebook, YouTube, Instagram, WhatsApp or TikTok, in the online games you play on your phone, tablet or computer, by chat or live conversations, via email or an online form.

3 **WHO?** The villain may be a malicious adult who pretends to be your online friend of the same age as you, an important person, relative or acquaintance. He will try to persuade you to tell your secret personal data. Or he may be lying that you will receive something super interesting (a phone, a new game) in exchange for information about you or your family.

4 **SHH, SECRET!** If villains obtain your secret personal data, they will be able to - for example – track you down at home or at school and harm you. Or create fake Internet accounts and pretend it's you!

PARENT'S PAGE

1. WHAT PERSONAL DATA? Make with your child a list of information that he/she should not disclose on the Internet – neither when asked, nor on his/her own initiative, in public conversations or posts. The rule of secrecy applies not only to his personal data, but also to that of friends and colleagues! Where possible (online games, social media platforms, quizzes etc.) strictly fill in the required fields, use a pseudonym, provide as little information as possible.

2. WHO GETS YOUR PERSONAL DATA? It may seem normal for the child to share all kinds of information with virtual friends. They're friends, aren't they? Explain that not everyone on the Internet is who claims to be, especially if we are talking about people he/she has had contact with exclusively online.
Even if someone looks in pictures, writes or behaves like a child, the little ones can be fooled. It is safest to understand that he/she must always be cautious and never give out personal information.

3. FRIENDS ON SOCIAL MEDIA. For certain social media platforms where this is possible, such as Facebook, Instagram or TikTok, it is good to be in the list of friends / followers of your child.
This will allow you to monitor text posts, photos, uploaded videos, and comments, and respond in a timely manner if they include personal data.
Also, on social media, choose the optimal privacy settings for the private child's account, not a public one. Limit the audience that can see the posted content and personal information (the less, the better) to the friends list.

4. WE LEARN FROM MISTAKES. Don't worry if your child makes a mistake, posting something he/she shouldn't. Help him/her delete the post and discuss together how to avoid a similar mistake in the future. If you overreact or deny access, they may not reach for your help anymore.

5. THE POWER OF EXAMPLE. We know you are proud of your child, but resist the temptation to post information, pictures or movies on social media, groups or online forums. For example, do not post photos or videos from the first day of school, with the addition of the location, or from the child's birthday, on the day of the event, with the age (or the number on the cake). Although personal data is not provided explicitly, it can be easily deduced. You are the first and best example for your child!