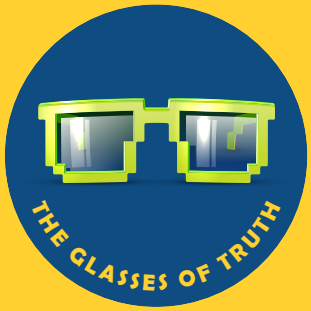
certSIGN

Cyber4Kids

LESSON 3.

Who is catfishing you? Fake identities

By following these cyber security tips, you will become a Cyber Superhero and you will activate a magical object – THE GLASSES OF TRUTH! This way you will be able to recognize the lies of villains who claim to be someone else online!



1. **ONLINE FRIENDS?** Beware of people who request your friendship or start talking to you through online messages on Facebook, YouTube, Instagram, WhatsApp, TikTok or in games chat rooms. There may be criminals who lie about who they are and their age, in order to harm you!

2. **WHY?** Cybercriminals who lie about who they are:
   • Want to laugh at you and make jokes about you – they steal the identity of a real person or invent one. They may even be children you know and pretend to be someone else.
   • Want to get your personal data and details about your family;
   • Want to get pictures and videos with you or they want you to meet in real life.

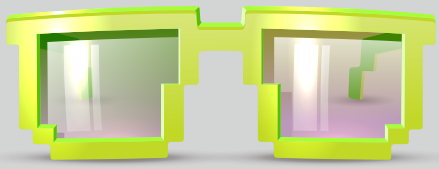
3. **HOW DO YOU AVOID THIS?** Always follow these tips:
   • Never accept friend requests or reply to messages / comments from strangers;
   • Never post online your personal data, pictures, videos or any other information about you and your family;
   • Don't believe everything that people who contact you online say;
   • Never respond to challenges thrown out by virtual friends, especially if they seem inappropriate and would make you feel uncomfortable;
   • Tell your parents about the people who talk to you online, especially if they tell you, send or ask you thinks that make you feel uncomfortable;
   • Never pretend to be someone else online, just to make a joke.

PARENT'S PAGE

1. TALK ABOUT FAKE IDENTITIES. Explain to your child that there are many people online who lie about who they really are (including about their age), often with malicious intent.
It is safest to never accept friend requests or reply to messages from strangers requesting personal data or pictures and videos with him/her until after consulting with you or another trusted adult (relative, an educator etc.).

2. TEAM OF DETECTIVES! Perform together false account recognition "exercises":
• Profile photo – its lack, a general or blurred image, the existence of a single portrait photo with the respective physiognomy are alarm signals;
• Profile age and content – a recently created account, with very few posts and interactions, biographical information missing, minimal or not found in other online searches, can be fake;
• Mutual friends – existence of a circle of mutual friends is essential. Even so, an online friend's friend remains a stranger;
• Verification in real life - in case of friendship requests received from people who claim to have heard of the child from someone else / are acquaintances of a third person, verify with the latter the reality of the information.

3. DANGEROUS MESSAGES. Give your child real examples of dangerous messages they don't need to respond to, such as:



• *"Hi, your posts are great, can you give me your phone number to talk on WhatsApp?"*
• *"Hey, I'm your classmate's / friend's brother (+ name from friends list). Can you give me your address? I have something to give you from her.*
• *"Your pictures / videos are great! Follow me and let's talk more!"*
• *"Hey, you like this picture of me? Give me one of yours."*

4. PRECAUTIONS. Always create together accounts on social media platforms, preferably be the first friend on the child's list and monitor as much as possible the posts and conversations, but also in chat rooms of online games.
Set accounts as private, limiting audiences who can send friend requests, direct messages, share, or comment to friends (or no one).
Block together users with inappropriate interactions and their messages.
Encourage the use of mobile devices and laptop / computer only for certain periods of time, in a common room where an adult is also present.