



Cyber4Kids

LESSON 1.

Mobile games, in safety

By following these cyber security tips, you will become a Cyber Superhero and you will activate a magical object – the VICTORY RING! This way you will be able to play safely on your mobile phone or tablet!



1

NEW GAME. It is best to install new games with your parents. They will tell you if they are right for you so you can play safely!

2

WHAT IS YOUR NAME? When choosing a name for the game, do not use your real name, age or date of birth.

3

ON THE CHAT. Some games have a chat section where you can write messages or have live conversations with other players. Don't forget to treat everyone nicely! If someone doesn't talk nicely to you, leave the conversation.

4

SECRET DATA. If another player asks what is your name, where do you live, what school you attend or asks to see you in a certain place, don't answer! This data is secret!

5

LINKS. Also, on the chat, you may receive links from other players – do not open them! Messages can be sent by undercover criminals and those links can be a trap!

6

ABOUT MONEY. When you play, you will surely see messages that offer you, in exchange for money, mega powers or a new weapon for your character! Some may promise to get rid of ads that interrupt your adventure. Decline and close these messages asking you to pay.



PARENTS' PAGE



Always check application/games, preferably before downloading and using them:

- beware of games listed on third-party platforms (apart from Google Play / App Store – the existence of malware applications is not ruled out here either, but the risk is much lower);
- always consult reviews – those containing more than two words and in natural language;
- search online for information about the game developer to verify its legitimacy.;
- use an antivirus solution for mobile security.



Set up parental control in Google Play/App Store to:

- block applications that you do not want your kid to use;
- block downloads and purchases, depending on the content maturity level;
- automatically lock the screen of the mobile device used by the child, for bedtime.



Always check the content rating (PEGI label - Pan European Game Information) and game reviews to make sure it's appropriate for your child's age.



Avoid accidental or unwanted purchases using protection by authentication (password/ PIN request before making any payment). Keep this data for yourself only.



Practical test - take a few minutes to personally "test" the game. You will have a new common topic to discuss, you will spend time together and the child will enjoy the interaction with you.



Talk frequently about the child's experience in the game, encouraging him/her to tell you if someone is verbally abusing him/her, asking for personal data, inappropriate images, or making him/her uncomfortable.



Consider disabling the webcam / microphone for games where this is possible.

