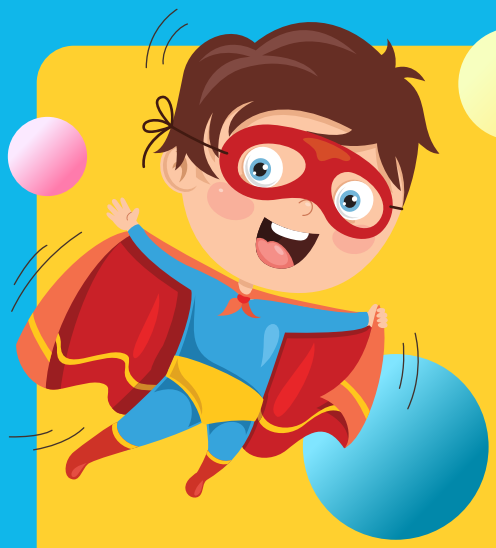


certSIGN

Cyber4Kids

LESSON 4.
Dangerous links

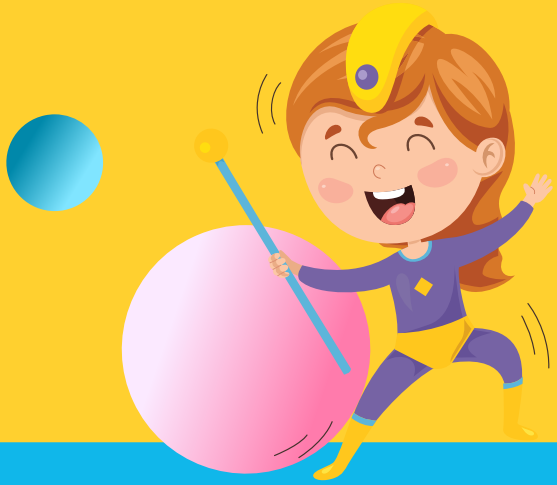
By following these cybersecurity tips, you will become a Cyber Superhero and you will activate a magical object – THE REALITY BRACELET! It will help you recognize false links, which hide viruses and cybercriminals.

1 **VIRUSES AND MALWARE.** Cyber criminals can send you links that hide viruses, malware and dangerous messages, which may damage your phone, tablet or computer or steal your personal data, without you realizing it.

2 **CLICK HERE!** To make sure you click, cybercriminals would lie and say that at that link you can watch or download a super funny video/game. Or they may promise you that if you go to that site and give them your personal data, you'll win a lot of money, a phone, a table, a toy, new powers in your favorite online game.

3 **HOW TO AVOID THIS?** Always follow these tips:

- **Do not click on any link** or on a link you received from unknown people;
- **Do not believe** messages that promise you will receive something valuable – nothing is free on Internet;
- **Do not download** games, music, movies or anything from sites or emails sent to you by strangers;
- **Check** that the links you have clicked have a closed padlock in front of the address - this means they are safe for you;
- **Do not provide personal data or passwords** on Internet sites, in online questionnaires, in response to e-mails or messages on the phone;
- **Ask your parents first** if it is OK to open a link or a site.



PARENTS' PAGE

1. RISKS. Explain to your child the risks of simply accessing a link / website or downloading an attachment that may lead to the automatic installation of malware on the used device. These actions can give other people access to his/hers phone, tablet or computer.

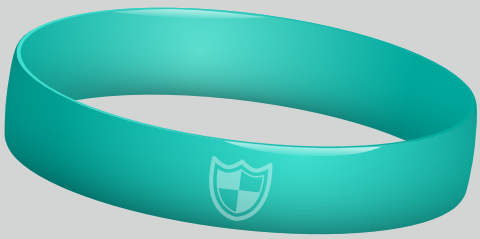
2. PRACTICAL TEST. Teach your child how to verify the authenticity of links, sites and e-mails received:

• **LINK.** It doesn't start with https:// but with http://? Is the small padlock in front of the URL missing (on the left)? **It is not safe.**

• **SITE.** The URL doesn't match the information displayed on the page (for example, in the site address the letters are replaced by numbers or the words are misspelled – c0npany)? Is the logo missing from the page? Are there many typos in the displayed text or is it written in very small letters? Are there many pop-ups? Does it say you won something? Does it request personal data? **It is not safe.**

• **E-MAILS.** You don't recognize the person/source who sent the message? Are you offered something for free or it lets you know that you won something? Did a friend send you the message online but when you verified with him/her in reality (mandatory) it didn't check? Does it ask for personal information or passwords? Are there many typos in the displayed text or is it very small? **It is not safe.**

3. ANTIVIRUS SOLUTIONS. Curiosity is natural for the little ones, as they are always attracted to new things and can easily access malicious links or download games from unknown websites. Therefore, installing an antivirus solution, which includes a real-time scanning engine, firewall and automatic update, is essential. Such a solution helps you against problems such as spyware and viruses on the sites that your child accesses.



Seemingly legitimate links / sites may contain malware or redirect to a fake site that looks the same, but actually contains a keylogger (a program that records every keystroke on a keyboard and saves this data in a file) or a virus.

Periodically perform automatic virus checks and deep system scans to make sure there are no unwanted "visitors" and that your child's personal information is not collected.

4. PARENTAL CONTROL SOLUTIONS. With the help of a parental control solution (both for mobile and desktop devices) you can monitor the child's Internet experience from the time allowed to spend online, to applications and websites used / accessed. Attempts to use blocked programs will be stopped and logged in the program log for later viewing.