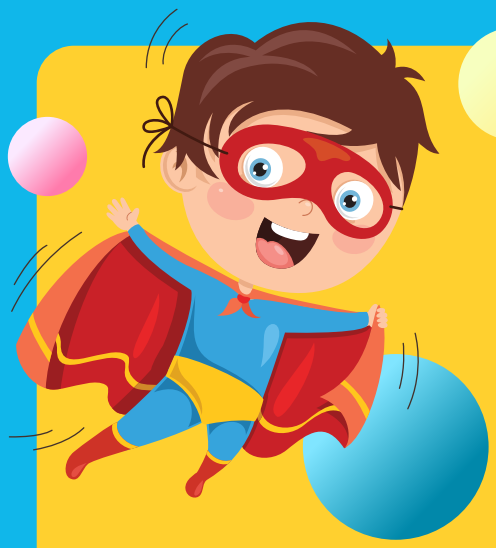


certSIGN

Cyber4Kids

LESSON 7.
WiFi or not WiFi?

By following these cyber security tips, you will become a Cyber Superhero and activate a magical object - the WAND OF TRUST! It will help you connect safely to the Internet and you will know which networks are right for you!

1 **ON THE INTERNET, THROUGH WIFI.** To access the Internet, all you have to do is connect online from your phone, tablet or computer. One of the doors you can access the Internet is the WiFi network. You use it at home, at school or in public places such as museums, parks, restaurants, shops, airports or hotels. Where only you and your family can connect to the WiFi network at home, to other networks anyone can have access. Including cyber criminals.

2 **HOW DO YOU PROTECT YOURSELF?** Always follow these tips:

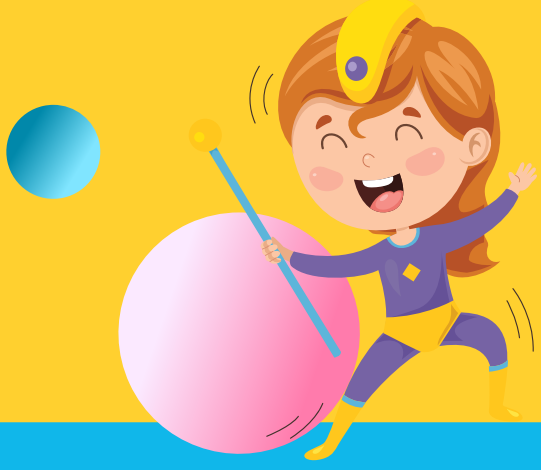
• **Be careful what WiFi you connect to.** Even if it includes the name of the location where you are, that network might have been created by a cybercriminal, or it might be a trap!

• **Public WiFi may not be safe.** Even if there is a key - a password to access them – even a cybercriminal might know it. It can even be the person at the table next to you, from a restaurant, who will be able to see what messages you are sending, discover your passwords or access your accounts.

• **Do not access from public WiFis websites that require your personal data.** You don't know who can see them when you're online using unsafe connections! Other people on the same network might see what you're sending and have access to your personal information, contacts, pictures, usernames and passwords.

• **Do not allow your phone, tablet or laptop to automatically connect to WiFi.** Ask your parents to turn off on your devices this feature.

• **Do not install applications or access unknown sites and links on public WiFi**. Make sure that the links you have entered have a closed padlock in front of the address and start with HTTPS.



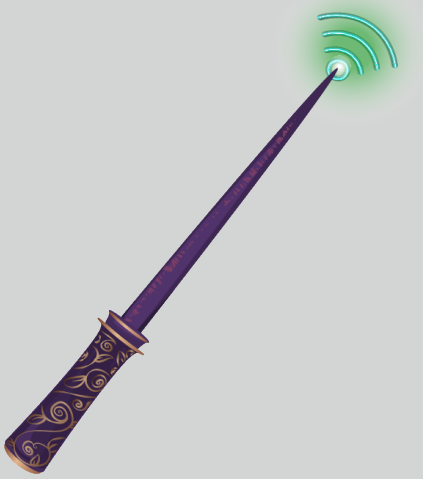
PARENT'S PAGE

1. PRIVATE, PUBLIC WIFI OR MOBILE CONNECTIONS? Explain to your child the differences between the means of connecting to the Internet: private WiFi at home (paid, secure, which can only be accessed by you by entering a secret password and not by neighbours), WiFi in public places such as museums, parks, restaurants, shops, airports or hotels (open to anyone who knows the password, when there is one, and not as secure) and mobile data (connection for phones, tablets, paid and limited, which may incur additional costs).

2. THE RISKS OF PUBLIC WIFI NETWORKS. In order for your little one to understand from you why it is not advisable to use free WiFi networks, you must first know what their risks are:

• **Man-in-the-Middle (MitM).** A MitM attack involves intercepting a communication between two systems, by an external third party. No matter what we're talking about (email, social networking, online browsing), cybercriminals can directly intercept communication when you connect to an unencrypted WiFi network, risking tampering with messages, stealing personal data, information on the device (passwords, banking information etc.).

• **Malware.** Attackers can trick you into downloading malicious content when you connect to public WiFi. The danger of malware (viruses, computer worms, spyware, adware, Trojans) can range from infecting devices, stealing personal information, viewing offline files such as photos and sensitive documents, to accessing the camera and microphone so that someone else knows what you're doing even in the real world, not only online.



• **Malicious Hotspot.** Cybercriminals can set up a hotspot in a public area, calling it "Public WiFi" or after a cafe, a store or the headquarters of a nearby company. While looking for a free internet connection, such a name may seem legitimate and you can easily become a victim of attackers who will spy on your online activity, without realizing that you are in danger.

3. SSL AND VPN IN CONTROL! Especially on public WiFi, SSL connections should be used (i.e. only those sites that include a closed padlock and **HTTPS** at the beginning of the links should be accessed). This protocol involves encrypting traffic between your device and a website, guaranteeing the authenticity of the latter and making it difficult for intruders to intercept communications.

It is also recommended that you use a Virtual Private Network (**VPN**) solution on all devices to secure Internet activity, encrypt traffic, and hide your IP address. The secure connection between you and the Internet created by this private virtual network is essential for the protection of personal data in the online environment.