certSIGN

Cyber4Kids

Cyber education textbook for children and parents

cyber4kids.ro

certSIGN

Cyber4Kids

TABLE OF CONTENTS

certSIGN

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 players 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.

Find out more on cyber4kids.ro!

certSIGN

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!

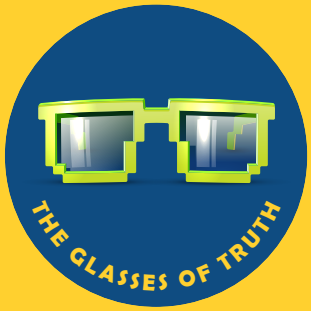
certSIGN

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.

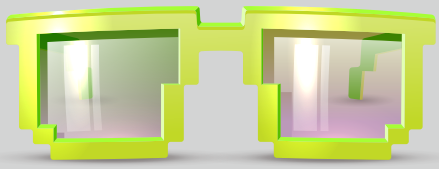
3. **HOW DO YOU AVOID THIS?** Always follow these tips:
   • Never accept friend requests or reply to messages / comments from strangers;
   • Never post online your personal data, pictures, videos or any other information about you and your family;
   • Don't believe everything that people who contact 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.

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.

certSIGN

Cyber4Kids

LESSON 5.
The Internet never forgets!

By following these security tips, you will become a Cyber Superhero and you will activate a magical object – THE DIARY OF ADVENTURES! You can log unforgettable memories and it will help you show others great things about you!

1. **THE INTERNET NEVER FOREGETS!** Even if you change or delete what you post online (comments, pictures and videos, messages, etc.), there will be people who have already seen what you published. Maybe they even downloaded, sent to someone else or took a screenshot (a picture) of what you posted. Deleting information from the Internet does not mean that it disappears forever!

2. **FUN!?** Posts that seem okay to you now may not seem as fun when you grow up. Neither to you nor to anyone else - because anyone will be able to find whatever you posted, 10 or even 20 years ago, judge you or laugh at you! Those who don't know you will be able to find online a lot of information about you and make a wrong opinion!

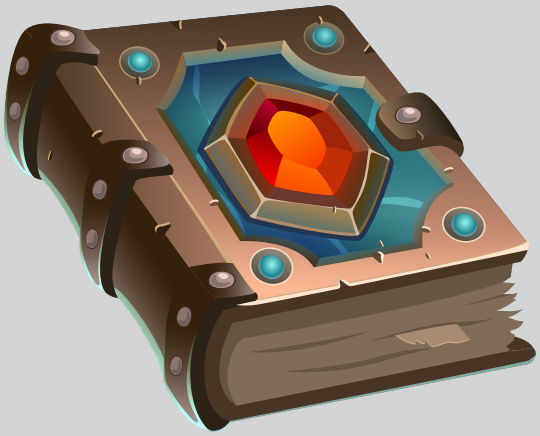
3. **WOULD I DO THIS IN REAL LIFE?** Each time you want to post something ask yourself whether:

• Would you make the same joke, use the same words, and say the same things about a person if you were face to face with them?
• Would the pictures and videos with you posted online seem fun to your parents as well? What do you do in them is fair and polite?
• Would you tell a stranger you meet on the street your name, where you live, information about your family, accept gifts and go with him anywhere?
If the answer is no, then do **NOT** do all this just because you are behind a phone, tablet or computer.

PARENTS' PAGE

1. WHAT YOU POST ONLINE (DIGITAL FOOTPRINT) MATTERS. Explain to your child the importance of a digital footprint - every online action is associated with a digital record, which is stored online for access at any time - by us and, most importantly, by anyone else.
From text posts and media files that aren't exactly "inspired" on social media, to personal data published and indexed online - every piece of information contributes to the way we are perceived, with potential negative repercussions in the medium and long term.
For example, multiple colleges and companies search the Internet before accepting candidates, and information about us can be found by any foreigner, more or less well-intentioned.
Maintaining a positive reputation both online and offline is essential!

2. WHY THE INTERNET NEVER FORGETS? Carry out a small test together so that your child understands the power of the Internet to remember - type in your name or that of a known person in a search engine and then browse the results together.
You will notice that a wide range of information is covered - from posts, images, videos, to comments and any other activities on websites.



However, the most important thing is to understand that removing this digital content can be from very simple (with a simple click on the "Delete" option) to very difficult (asking search engines or website owners to do it), to the point of impossibility - we have almost no control over how the online community uses our published data and content (who downloads, copies or makes it available elsewhere).

3. IS IT REALLY FUN? There are many situations in which posting certain photos, videos or comments had negative effects for their "owners". The impulses of the moment and the opinions of the past can turn against us in a few years.
Some edifying examples in this regard, which can be given to the child, to better understand the risks to which he / she is exposed when posting anything, without applying a "filter":
• images or movies published on social channels in various ways that do not benefit him / her, socially unacceptable or out of context (gone viral, turned into memes, digitally processed);
• insulting posts or vulgar language.

certSIGN

Cyber4Kids

LESSON 6.
Cyberbullying

By following these cyber security tips you'll become a Cyber Superhero and activate a magical object – the AMULET OF FRIENDSHIP! It will protect you from those who mistreat you online!

1 **WHAT IS CYBERBULLYING?** When someone misbehaves online, becoming a bully - a person who wants to upset you or laugh at you.

For example, he writes annoying messages or threatens you, tells lies about you or gives you mean nicknames, and even urges other people to bully you.

Or try to fool others online by pretending to be you and posting offensive information, photos or videos without your knowledge or consent.

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

- **talk to a friend but most importantly to a trusted adult** - your parents, a relative, the teachers can help you;
- **do not reply to messages, comments or posts from bullies** – if someone upset you, it is possible to say things you'll regret later;
- **block and report bullies** – they will no longer be able to send or post unpleasant things;
- **gather evidence** – keep, by saving or taking a screenshot, the malicious emails, messages, images or videos you receive and show them to your parents;
- **always reconsider what you post online** – bullies can use what you posted against you, or forward to others and make fun of you. And don't post anything that could hurt someone;
- **do not appreciate or forward** messages or posts in which someone laughs at a person or says bad thinks about them – if you do that, you become a bully too;
- **never tell the passwords to your account** – even children who seem to be your friends could use them to access your accounts, post unpleasant things or send malicious massages on your behalf.

PARENTS' PAGE

1. COMMUNICATION IS ESSENTIAL! Constantly encourage your child to talk to you about online experiences and let them know that they can turn to you for any problem, every time something that upsets them happens or makes them uncomfortable. And for the "backup option" (despite our openness and effort, it may be easier for the little ones to talk to someone else) tell them that it's ok to talk to someone both of you trust (a friend, relative, educator).

2. "IT'S OK, IT WILL PASS!" IS NOT A SOLUTION. Cyberbullying can make children feel ashamed and withdraw into themselves, with real mental (sadness, anger), emotional (apathy, loss of interest in things they used to like) and even physical effects (fatigue, insomnia), which in extreme cases can lead to suicide. By communicating openly and paying close attention to cyberbullying, you can help your child regain his trust and wellbeing.

3. REPORT, BLOCK, PROVE. Social media platforms (TikTok, Facebook, YouTube, Intsagram, WhatsApp) allow blocking and reporting of users and / or content and comments posted by them. In cyberbullying situations, you either carry out these processes with the little one, or you teach him how to report and block the bullies and their messages on their own. Also, collecting evidence (text messages and screenshots of social media posts, including media files) can be useful in the long run to demonstrate aggressions.

4. PREVENTIVE MEASURES. As much as possible, monitor the child's online activity, respectively the comments received on what he posts. For its protection, in online accounts the privacy settings must be those of a private account, limiting only to the list of friends the audience that can see what they post and comment or send messages.

5. THE FACESE OF CYBERBULLYING. The fear that the little one will become a victim of cyberbullying is founded nowadays, but do not forget that there are also the roles of **bully** or **witness**. The child needs to understand that cyberbullying is not fun and not every action or word said online can fall into the "It was a joke!" category. The main message? To treat others as he/she would want others to treat him/her!

And if he/she is witnessing a case of cyberbullying - whether the victim is a known person or not - not to become an accomplice witness encouraging the bully's behavior (through distribution, likes, etc.), but to be a protective witness (to support the victim with messages of support, to report the bullying / bully).

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.

certSIGN

Cyber4Kids

LESSON 8.
Magical passwords

Following these cybersecurity tips, you will become a Cyber Superhero and activate a magical object - THE CHEST OF WISDOM! In it you can safely keep mega-strong passwords, which no cybercriminal will discover!

1. **STRONG PASSWORDS.** Do not use simple words (eg Minecraft, chocolate, StarWars) or consecutive numbers (123456) in passwords. And NO, the word "password" is not a good password at all! A strong password must be longer, at least 8 characters, and more complicated. Mix in uppercase and lowercase letters, numbers and symbols.

2. **FUNNY PASSWORDS.** Take out the first letters of each word from a funny sentence you create, which you can easily remember, and enter numbers and symbols. For example, from the sentence "The rabbit and the cat saw two movies at Cinema" you will get this mega strong password – **Tr&tcs2m@C**.

T	r	&	t	c
The	rabbit	and	the	cat
s	2	m	@	C
saw	two	movies	at	Cinema

3. **NO PERSONAL DATA.** Do not include in your passwords your name, date of birth, parents' name, telephone number or any other personal data that others may know or guess.

4. **SECRET PASSWORDS.** Don't tell your passwords to anyone except your parents! Even your best friends might be tempted to make a joke and use them to access your accounts, pretending to be you. And never write down passwords in a place that is easy for someone else to find (notebooks, post-its, etc.).

5. **DIFFERENT PASSWORDS.** Don't use the same password everywhere! It is good to have a different one for each account (games, Facebook, YouTube Instagram, TikTok or email). Using the same password for multiple accounts is like having the same key for each door. If a cybercriminal steals or copies the key, each door (account) will be vulnerable.

PARENTS 'PAGE

1. "THREE LITTLE PIGS", PASSWORD VERSION. To better understand the differences between a weak, a medium and a strong password, respectively the importance of the latter, you can explain these things to your child using the reinterpretation of a story (a movie or real-life situations - according to your inspiration and imagination). We propose "The three little pigs", in which the wolf becomes the cybercriminal and the three houses built become:

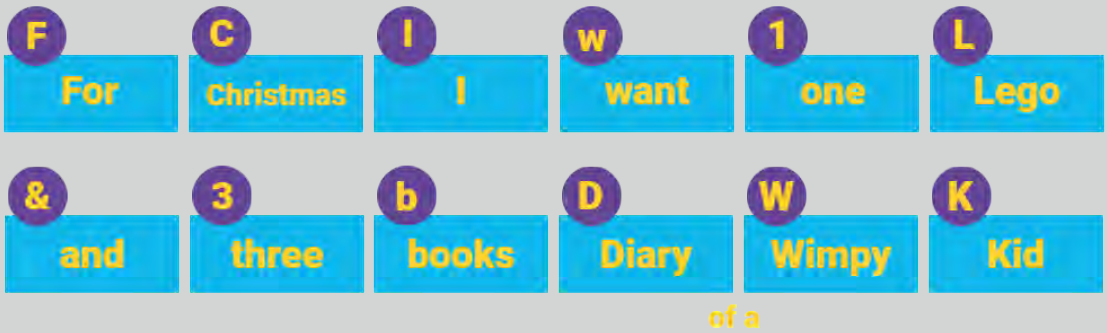
• **weak password** (straw house) - extremely easy to break or guess. Examples: password123, qwerty, andrew111;

• **medium password** (twigs house) - a higher degree of difficulty, but not impossible to guess, whether we are talking about people who know the child or malicious software (keylogger, screen scraper) used by cybercriminals. Example: ILoveLego, Andrew2o2o;

• **strong password** (stone and brick house) - a high degree of difficulty, allowing to keep accounts and personal information safe. Example: Ilg@C&sHPm, FCIw1L&3bDWK.

2. THE GAME OF MAGICAL PASSWORDS. Turn the creation of strong passwords (several, different for each account) into a game that you play together periodically - passwords should be changed at least once every 6 months. Let the child come up with simple and funny sentence ideas that he/she can easily remember, and then guide him/her on how to get strong passwords by extracting the first letter of each word and inserting numbers and symbols.

We got the above examples from the sentences "I like going to Cinema and see Harry Potter movies" (Ilg@C&sHPm) and "For Christmas I want one Lego and three books Diary of a Wimpy Kid" (FCIw1L&3bDWK). And change the passwords for Easter!



3. BUT IT'S MY PASSWORD! It is very possible that your kid will not understand why you should know his/her passwords (after all, they should be secret, shouldn't they?). Or he/she will not be happy that you will have access to his/her online activity. Make your child understand that his safety, including in the virtual environment, is your duty as a parent.

And just because you have the passwords for his accounts, it doesn't mean you'll use them to keep track of everything he /she does online. In fact, even at home, the child can keep the door of his room closed and you could knock before entering. But it is not permissible for you, as a parent, not to have access.

certSIGN

Cyber4Kids

Video

Welcome to Cyber City!
(ep. 0) | [EN Sub]

We play safely
(ep.1) | [EN Sub]

Personal secret data
(ep.2) | [EN Sub]

Fake identities
(ep.3) | [EN Sub]

Dangerous links
(ep.4) | [EN Sub]

Internet never forgets
(ep.5) | [EN Sub]

Cyberbullying
(ep.6) | [EN Sub]

WiFi or not WiFi?
(ep.7) | [EN Sub]

Magical passwords
(ep.8) | [EN Sub]

youtube.com/certsign